

Assurance report

Bizbrains A/S

Independent auditor's ISAE 3000 Type I assurance report with limited assurance on measures for risk control related to network- and information systems and reporting obligations according to agreement with customers throughout the period from 2 November 2025 to 31 August 2026

November 2026

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Penneo document key: D1HON-NAV3Y-IR58C-4

Table of contents

Section 1:	Bizbrains A/S' statement	1
Section 2:	Independent service auditor's ISAE 3000-II assurance report with limited assurance on measures to manage risks in relation to network and information systems and reporting obligations pursuant to the agreement with customers	3
Section 3:	Bizbrains A/S' description of NIS2 related services regarding the delivery of the Link 3 platform	5
Section 4:	Control objectives, control procedures, assessment and results of assessments	9

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Section 1: Bizbrains A/S' statement

Bizbrains A/S (the NIS2 Service Provider) provides services to customers in accordance with the NIS2 service provider agreement throughout the period from 2 November 2025 to 31 August 2026.

The accompanying description has been prepared for customers, who has used Bizbrains A/S' services in regard to the Link 3 platform, and who has a sufficient understanding to consider the description along with other information, including information about controls operated by customers itself when assessing whether the requirements to ensure a high level of cyber security under applicable law have been complied with.

Bizbrains A/S uses A/S ScanNet and Microsoft Inc. as NIS2 subservice providers. The assurance report uses the carve-out method and excludes control objectives and related controls that A/S ScanNet and Microsoft Inc. operates for Bizbrains A/S.

Some of the control objectives stated in Bizbrains A/S' description in Section 3 can only be achieved if the complementary user entity controls at customers and A/S ScanNet and Microsoft Inc. are suitably designed, implemented and operating effectively together with the controls of Bizbrains A/S. This report does not extend to cover the suitability of the design, implementation and operating effectiveness of these complementary user entity controls.

Bizbrains A/S confirms that:

The accompanying description, in Section 3, appropriately presents Link 3 platform, which has been used by customers throughout the period from 2 November 2025 to 31 August 2026. The criteria used in making this assertion were that the accompanying description:

(i) Presents how Link 3 platform was designed and operationally effective, including:

- The types of services provided
- The processes in network and information systems used to provide the services
- How network and information systems process significant events other than those directly related to the provision of services
- The processes directed to support, in the event of any breach of security regarding services, that customers can report such breach to the regulatory authority
- The processes directed at events that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems
- Relevant control objectives and controls designed and operated effectively to achieve those objectives
- Complementary user entity controls that we, in reference to the scope of Link 3 platform, have assumed would be implemented by customers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description
- Other aspects of our control environment, risk assessment process, information system (including related business processes) and communication, control activities, and monitoring controls that are relevant to the provision of services.

(II) Includes relevant information about material changes in Link 3 platform made throughout the period from 2 November 2025 to 31 August 2026

(iii) Does not omit or distort information relevant to the scope of Link 3 platform, taking into consideration that the description was prepared to meet the general needs of a wide range of customers and may not, therefore, include every aspect of Link 3 platform that the individual customer may consider important in its own particular environment.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and operationally effective throughout the period from 2 November 2025 to 31 August 2026. The criteria used in making this assertion 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 assurance that those risks did not prevent the stated control objectives from being achieved; and

   (III) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 2 November 2025 to 31 August 2026

c) Appropriate and proportionate technical, operational and organisational measures were established and maintained to manage the risks posed to the security of network and information systems for the provision of services to customers and to prevent or minimise their impact.

It should be pointed out with respect to the above assessments that the regulations regarding the requirements for security in network and information systems are new and complex. A consistent practice for how to interpret the individual rules has yet to evolve in all areas. Although we believe that we have established and maintained appropriate and proportionate technical, operational and organisational measures, circumstances may therefore prove to exist causing authorities and business partners to take a different view.

Copenhagen, 3 November 2026
Bizbrains A/S

Mads Vigh
CEO

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Section 2: Independent service auditor's ISAE 3000-II assurance report with limited assurance on measures to manage risks in relation to network and information systems and reporting obligations pursuant to the agreement with customers

To: Bizbrains A/S and their customers

Scope

We were engaged to provide assurance about Bizbrains A/S' description in Section 3 of the Link 3 platform in accordance with the NIS2 service provider agreement throughout the period from 2 November 2025 to 31 August 2026 and about the design, implementation and operating effectiveness of controls related to the control objectives stated in the description. This assurance report concerns whether Bizbrains A/S designed suitable controls and whether those controls have been operated effectively throughout the period from 2 November 2025 to 31 August 2026 related to the control objectives stated in Section 3. The assurance report does not include any assessment of Bizbrains A/S' general compliance with the requirements of the EU Directive on measures for a high common level of cyber security across the Union. Bizbrains A/S uses A/S ScanNet and Microsoft Inc. as NIS2 subservice providers for the deliverance of the Link 3 platform. The assurance report uses the carve-out method and excludes control objectives and related controls that A/S ScanNet and Microsoft Inc. operates for Bizbrains A/S. Some of the control objectives stated in Bizbrains A/S' description in Section 3 can only be achieved if the complementary user entity controls at customers and A/S ScanNet and Microsoft Inc. are suitably designed, implemented and operating effectively together with the controls of Bizbrains A/S. This assurance report does not extend to cover the suitability of the design, implementation and operating effectiveness of these complementary controls.

We express limited assurance in our conclusion.

Bizbrains A/S' responsibilities

Bizbrains A/S is responsible for preparing the description and accompanying assertion in section 1, including the completeness, accuracy and method of presentation of the description and assertion, for providing the services covered by the description, for stating the control objectives, and for designing, implementing and effectively operating controls to achieve the stated control objectives.

Grant Thornton's independence and quality management

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark. Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express a conclusion, based on our procedures, on Bizbrains A/S' description and on the design, implementation and operating effectiveness of controls related to the control objectives stated in that description. We conducted our engagement in accordance with International Standard on Assurance Engagements ISAE 3000, "Assurance Engagements other than Audits or Reviews of Historical Financial Information", and the additional requirements under Danish audit regulation in order to obtain limited assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed, implemented and operating effectively.

A limited assurance engagement to report on the description, design, implementation and operating effectiveness of controls at an NIS2 service provider involves performing procedures to obtain evidence about the disclosures in the NIS2 service provider's description of their service, and about the design, implementation and operating effectiveness of

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not adequately presented, and that controls are not suitably designed, implemented or operating effectively. Our procedures included analyses, inquiries and other procedures to obtain limited assurance about our assessment of the operating effectiveness of those controls that we consider necessary to provide limited assurance that the control objectives stated in the description were achieved. A limited assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the relevance of the criteria specified and described by the NIS2 service provider in Section 1. The procedures in a limited assurance engagement are different in nature and timing, and are less in extent, from a reasonable assurance engagement. Consequently, the level of assurance obtained for our opinion is significantly lower than would have been obtained in a reasonable assurance engagement.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at an NIS2 service provider organisation

Bizbrains A/S' description is prepared to meet the common needs of customers and may not, therefore, include every aspect of the services and control activities related thereto that customers may consider important in its particular environment. Also, because of their nature, controls at a NIS2 service provider organisation may not prevent or detect all breaches of cyber security. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at an NIS2 service provider organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this assurance report. The criteria we used in forming our opinion are those described in the Management's statement Section 1. During the audit work, we have not found any material aspects, which would lead us to form the opinion:

(a) that the description of the Link 3 platform as designed and implemented throughout the period from 2 November 2025 to 31 August 2026, has not been appropriately presented, in all material respects, and

(b) that the controls related to the control objectives stated in the description were not suitably designed and implemented, in all material respects, throughout the period from 2 November 2025 to 31 August 2026

(c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, operated throughout the period from 2 November 2025 to 31 August 2026

Description of the assessment of controls

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

Intended users and purpose

This assurance report and the description of the assessment of controls in section 4 are intended only for customers, who has used Bizbrains A/S' Link 3 platform. We have assumed that customers has a sufficient understanding to consider it along with other information, including information about controls operated by customers itself when assessing whether the requirements to ensure a high level of cyber security under applicable law have been complied with.

Copenhagen, 3 November 2026

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Martin Brogaard Nielsen
Partner, CISA, CIPP/E, CRISC

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Section 3: Bizbrains A/S' description of NIS2 related services regarding the delivery of the Link 3 platform

The purpose of this description is to provide information to Bizbrains A/S' customers and their stakeholders (including auditors) about measures to manage risks in relation to network- and information systems and reporting requirements pursuant to agreements with customers.

Further, the purpose of this description is to provide information about NIS2 related controls, technical and organisational measures, and responsibilities between the entities covered by NIS2 (our customers) and Bizbrains A/S.

Processes and system setups etcetera individually agreed with Bizbrains A/S' customers are not included in this report.

Introduction

Bizbrains is an iPaaS company and consultancy firm specialising in assisting customers in exchanging EDI data between B2B relationships and applications. The Link 3 platform is used for exchanging EDI documents and conducting B2B integration. The Link 3 platform, operations and product development is in scope for the NIS2 compliance.

Description of services

From tracking data, to managing partners and solving errors, Link 3 puts you in control.

The Link 3 iPaaS can transfer documents over various protocols and document formats. Bizbrains recommends conducting document transfers through secure protocols such as SFTP, AS2, AS4, etc.

Control environment

At Bizbrains, compliance and security is among our highest priorities, which is why we strive in being ISO 27001, GDPR and NIS2 compliant by implementing the following:

- Management approved policies:
  - Information security policy
  - Risk management policy and procedure
  - Link 3 IPaaS risk assessment
  - Bizbrains IT contingency plan
  - Cryptographic control and encryption policy
  - Bizbrains' business continuity management policy and procedure
  - Supplier information security policy and procedure
  - Awareness training
- Important technical controls related to the NIS2 service:
  - DDOS protection
  - Multilayered backup systems and disaster recovery setups
- Internal controls for securing compliance:
  - Change management
  - Risk management for Link 3's core developed features, changes and vendors
  - RBAC access and PAM access control
  - Separation of duties and separation of production and test environments
- Monitoring of the control environment
  - 24/7 SOC and Incident management
  - 24/7 IT guards on duty handling alerts on the Link 3 iPaaS.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Risk management

The risk management policy and procedure for Bizbrains A/S, offers a structured approach to identifying, assessing, and addressing risks across our operations. The risk management establishes a consistent framework for managing risks based on the ISO 27005 standard on risk management. It defines roles, responsibilities, and methods to ensure the protection of our assets and the continuity of critical activities. It is designed to support informed decision-making and align risk management practices with organisational objectives and obligations.

The accompanying procedure details the specific steps to implement the policy effectively, ensuring that risks are systematically addressed through clear and actionable processes. By integrating with relevant tools and systems, the procedure enhances efficiency and promotes consistency in risk management practices. Together, the policy and procedure serve as the foundation for managing risks and safeguarding the organisation's ability to achieve its mission and goals, regardless of specific regulatory requirements.

Control objectives and control procedures

Bizbrains A/S' IT security governance is based on the ISO27001/2 and ISO 27005 standard. Below is a description of the control objectives and the related control procedures that have been considered relevant for network and information systems in relation to the delivery and operation of Link 3 iPaaS.

Policies on risk analysis and information system security

Formalised policies and procedures are in place to ensure that sufficient guidance, roles, and responsibilities are established to support a structured and formalised process for identifying risks and embedding information security within the organisation. The following controls and procedures are in place:

- Information security policy
- Security procedures for IT department
- Risk management policy and procedure (NIS2 & ISMS)
- Link 3 IPaaS risk assessment
- Secure software development policy (NIS2)

Incident handling (prevention, detection, and response to incidents)

Formalised procedures and controls are in place to ensure timely and proper handling, including the detection, resolution, and reporting of incidents to customers. The following controls and procedures are in place:

- Procedure for incident management
- 24/7 SOC and incident management
- 24/7 IT guards on duty handling alerts on the Link 3 iPaaS.

Business continuity, such as backup management, disaster recovery and crisis management

Formalised procedures and controls are in place to ensure continued operations and the availability of services in the event of a disaster. The following controls and procedures are in place:

- Master disaster recovery plan.
- Bizbrains' IT contingency plan
- Bizbrains' business continuity management policy and procedure

Supply chain security, including security-related aspects concerning the relationships between the company and its direct suppliers or service providers

Formalised procedures and controls are in place to ensure that relevant and direct service providers (including subcontractors) throughout the supply chain are identified and monitored to ensure compliance with the company's security requirements and service delivery agreements.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

The following controls and procedures are in place:

- Supplier information security policy and procedure

The following key subcontractors are relevant for the delivery of our NIS2-related services:

- Microsoft
- A/S ScanNet
- ITM8 A/S
- Ontinue

Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure

Formalised procedures and controls are in place to ensure that critical assets are properly developed, maintained, and protected against vulnerabilities to internal and external threats.

The following controls and procedures are in place:

- Inventory of assets
- Network security features and expected services
- Network diagram
- Encryption policy and procedure
- Security procedures for IT department
- Secure software development policy (NIS2)
- Logging and monitoring policy and procedure

Policies and procedures to assess the effectiveness of cybersecurity risk-management measures

Formalised procedures and controls are in place to ensure that cyber-related risks and threats are identified, monitored, and remediated in a timely manner. The following controls and procedures are in place:

- Network security features and expected services
- Risk management policy and procedure (NIS2 and ISMS)
- Penetration testing
- Procedure for vulnerability scans

Basic cyber hygiene practices and cybersecurity training

Formalised procedures and controls are in place to ensure that cyber hygiene practices are implemented within the company and that employees undergo continuous training and education in cybersecurity. The following controls and procedures are in place:

- Training and awareness procedure

Policies and procedures regarding the use of cryptography and, where appropriate, encryption

Formalised procedures and controls are in place to ensure that critical assets are protected through encryption. The following controls and procedures are in place:

- Information classification policy
- Encryption policy and procedure

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Human resources security, access control policies and asset management

Formalised procedures and controls are in place to ensure that personnel security, access control, and asset management are structured, formalised, and maintained to ensure an appropriate level of security. The following controls and procedures are in place:

- Procedure for employees on and offboarding
- Access control policy
- IT-security policy
- Roles and responsibilities policy
- Equipment, seating and protection policy

The use of multifactor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the company, where appropriate

Formalised procedures and controls have been implemented to ensure a strong authentication process for managing access to critical assets, as well as secure emergency communication. The following controls and procedures are in place:

- MFA procedure
- Bizbrains IT contingency plan

Complementary user entity controls

The customer is responsible for the following:

- Customers need to ensure secure protocols are used in Link 3 when transmitting data
- Customers need to risk assess their own mappings and customer specific developed artifacts

Complementary subservice organisations controls

These key NIS2 subservice providers are responsible for the following:

- Microsoft – Hosting of IaaS platform such as Virtual network, virtual machines and Kubernetes primarily for services like SQL and container orchestration
- ScanNet – Hosting of IaaS platform such as Virtual network, virtual machines and Kubernetes primarily for services like SQL and container orchestration
- ITM8 – Hosting of IaaS platform such as Virtual network, virtual machines primarily for shared services like FTP
- Ontinue – 24/7 Managed Security Operations Center

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Section 4: Control objectives, control procedures, assessment and results of assessments

We have conducted our engagement in accordance with ISAE 3000, assurance engagements other than audits or review of historical financial information.

Our assessment of the implementation has included the control objectives and attached controls, selected by management and which are stated in the control objectives 1-10 below. Our assessment has included the controls; we find necessary to establish limited assurance for compliance with the articles stated throughout the period from 2 November 2025 to 31 August 2026.

This statement does not include control objectives and accompanying controls with A/S ScanNet and Microsoft Inc.

We have performed our assessment of controls at Bizbrains A/S by the following actions:

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

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control Objective 1: Policies on risk analysis and information system security

Formalised policies and procedures are in place to ensure sufficient guidance, role and responsibilities are established to support a structured and formalised process to identify risks and to anchor information security in the organisation.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Result of test*
1.1	A formalised organisational structure around roles and responsibilities for providing NIS2 services has been defined and implemented within the company.	We have inspected that a formalised procedure for roles and responsibilities exists in accordance with the delivery of NIS2 services. We have inspected that the actual roles and responsibilities are in compliance with the procedure.	No deviations noted.
1.2	The company has prepared and implemented a policy for information security in network- and information systems. The policy is approved by the management and communicated to all relevant stakeholders (internal/external), including the company's employees. Assessments are made on a regular basis – and at least once a year – as to whether the information security policy should be updated based on new information from the relevant authorities or/and changes in risk scenarios.	We have inspected that the information security policy is approved by management and communicated to relevant stakeholders. We have inspected documentation confirming that regular assessments are carried out, at least once a year, to determine whether the information security policy needs to be updated.	No deviations noted.
1.3	The Information security policy sets out guidelines for incorporation of information security requirements driven from internal as well as external mechanisms such as business strategy, GDPR and NIS2 regulation. Compliance with the policy is ensured through internal and external reviews.	We have inspected that the information security policy describes information security requirements mandated by both internal requirements and external regulations. We have inspected that compliance with the information security policy has been reviewed internally/externally.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control Objective 1: Policies on risk analysis and information system security

Formalised policies and procedures are in place to ensure sufficient guidance, role and responsibilities are established to support a structured and formalised process to identify risks and to anchor information security in the organisation.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Result of test*
1.4	A risk assessment is performed based on requirements from/to customers/service providers and following an industrial well-known standard/approach where each identified risk is assessed from a NIS2 perspective.	We have inspected that the process for conducting risk analyses is formalised and approved by management. We have inspected that the risk analysis has been carried out from a NIS2 perspective, follows requirements from/to customers and suppliers, and is based on industry standards/approaches.	No deviations noted.
1.5	The formalised process ensures that the risk assessment include the following activities: • Risk identification; find, recognise and describe the risk • Risk analysis: determine the causes/sources of the risk, the likelihood, consequence and severity	We have inspected that the risk analysis includes the following activities: • Risk identification: finding, recognising, and describing the risk • Risk analysis: determining the cause/source of the risk, the likelihood, the consequence, and the severity	No deviations noted.
1.6	Consequence criteria are developed considering the extent of damage or loss or harm to the company and/or the critical infrastructure in the community from the loss of availability of information/services perspective.	We have inspected that impact assessments have been prepared regarding loss and damage to the organisation and/or the critical infrastructure in society as a result of loss of availability of information and/or services.	No deviations noted.
1.7	The company continuously updates the risk assessment and the risk treatment on a regular basis at least annually and in case of changes.	We have inspected that risk assessments are reviewed and, if necessary, updated annually. We have inspected that risk assessments are updated and approved by management on an annual basis.	No deviations noted.
1.8	The management (Board of Directors/Risk committee etc.) are monitoring the identified risks, progress in mitigation actions and the general threat landscape on an ongoing basis (e.g. monthly/ quarterly).	We have inquired about how management monitors the identified risks. We have inspected that management continuously monitors the identified risks, the progress of mitigating actions, and the overall threat landscape.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 2 – Incident handling (prevention, detection, and response to incidents

Formalised procedures and controls are in place to ensure timely and proper handling, including detection, resolution, and reporting of incidents to customers.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
2.1	Management responsibilities and procedures are established to ensure quick, efficient and planned handling of information security incidents related to NIS2 services. The procedure contains specific prioritisation and time frame for handling information security incidents and communication channels.	We have inspected that management's responsibility for handling information security incidents is defined. We have inspected that a formal procedure has been designed and implemented to ensure the prompt, effective, and planned handling of information security incidents related to NIS2 services. We have inspected that the formal procedure includes information on: • Prioritisation • Timeframes for handling security incidents • Communication channels	No deviations noted.
2.2	An incident response plan has been prepared, and frameworks have been established for handling major information security incidents, which must be resolved within a set time frame.	We have inspected that a plan exists to ensure proper and timely handling of significant information security incidents.	No deviations noted.
2.3	An ITSM tool or similar is used for efficient handling documentation and reporting of information security incidents.	We have inquired about the process for registering and reporting information security incidents. We have inspected that an ITSM tool or equivalent has been implemented and is used for handling, documenting, and reporting information security incidents.	No deviations noted.
2.4	A management monitoring control is in place to ensure information security incidents are resolved within predefined time and in accordance with management expectations.	We have inquired about management's monitoring of information security incidents. We have, by sample test, inspected that information security incidents have been resolved within the set timeframe and in accordance with management's expectations.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 2 – Incident handling (prevention, detection, and response to incidents Formalised procedures and controls are in place to ensure timely and proper handling, including detection, resolution, and reporting of incidents to customers.			
No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
2.5	If any information security incident occurs which could have effect on NIS2 compliance, the company informs the customers and relevant authorities without undue delay and no later than the agreed timeframe after having become aware of such information security incident.	We have inspected the procedure for communicating to customers regarding information security incidents that affect compliance with NIS2 requirements. We have, by sample test, inspected that information security incidents have been communicated to customers without significant delay and within the set timeframe.	No deviations noted.
2.6	The company performs regular tests of the information security incident reporting process at least annually.	We have inquired about the procedure for regular reporting of information security incidents. We have inspected that the information security incident reporting process is tested at least annually.	No deviations noted.
2.7	The company has established and maintains a procedure, including baselines for audit logs.	We have inspected that a formalised procedure exists describing the baseline in relation to the configuration, collection, protection, and monitoring of logs.	No deviations noted.
2.8	Logs are configured in systems, databases and network components for following areas: • Activities performed by system administrator and other users with privileged access • Security events including changes in log-settings, including deactivation of logs, changes in user's access rights and failed login attempts to systems, databases and network components.	We have inspected that a formalised procedure exists describing the baseline in relation to the configuration, collection, protection, and monitoring of logs. We have, by sample test, inspected that the following are logged and monitored in relation to systems, databases, and networks: • User activities related to system administrators or other users with elevated privileges • Security incidents, including changes in log configurations, changes in user rights, failed logins, or multiple login attempts to systems, databases, and networks are logged and monitored.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 2 – Incident handling (prevention, detection, and response to incidents

Formalised procedures and controls are in place to ensure timely and proper handling, including detection, resolution, and reporting of incidents to customers.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
2.9	Logs are protected against manipulation/technical errors and are reviewed periodically.	We have inspected that a formalised procedure exists describing the baseline in relation to the configuration, collection, protection, and monitoring of logs. We have, by sample test, inspected on a system and database that log data are protected against manipulation and forwarded to a syslog server.	No deviations noted.
2.10	There is monitoring for systems and databases with an alarm feature that is generated by relevant events.	We have inspected that a formalised procedure exists describing the baseline in relation to the configuration, collection, protection, alerting, and monitoring of logs. We have, by sample test, verified that monitoring with an alarm function is set up on systems and databases, which is activated in the event of relevant incidents.	No deviations noted.

Control objective 3 – Business continuity, such as back management, disaster recovery and crisis management

Formalised procedures and controls are in place to ensure continued operation and availability of services in case of disaster.

No.	*Bizbrains A/S' control activity*	*Grant Thorntons performed test*	*Test result*
3.1	The company has implemented a formalised and approved business continuity plan that includes description of a resilient technical infrastructure, establishment of a crisis management capacity, coordination and maintenance of business continuity plans and measures.	We have inspected that a formal and management-approved contingency plan has been established, and that it includes the establishment of a resilient technical infrastructure, the development of crisis management competencies, and the coordination and maintenance of contingency plans. We have inspected that the technical infrastructure and crisis management resources are tested at least once a year.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 3 – Business continuity, such as back management, disaster recovery and crisis management

Formalised procedures and controls are in place to ensure continued operation and availability of services in case of disaster.

No.	*Bizbrains A/S' control activity*	*Grant Thorntons performed test*	*Test result*
3.2	Business continuity plan is developed and documented to support NIS2 related services. These plans describe the procedures to respond, recover, resume, and restore to a pre-defined level of operation for the related services. The business continuity plan is tested minimum annually.	We have inspected that the contingency plan includes procedures for how to respond, restore, and resume to a predetermined service level for NIS2 services. We have inspected that the contingency plan is tested at least once a year.	No deviations noted.
3.3	The company has determined requirements for information security and information security continuity in critical situations, for example in the event of a crisis or disaster.	We have inspected that an IT crisis management plan exists. We have inspected that the IT crisis management plan includes requirements for information security in the event of a crisis.	No deviations noted.
3.4	A management approved backup procedure is established. The procedure includes the frequency of backup, location, monitoring controls to address failures of scheduled backups.	We have inspected that a formalised backup procedure exists. We have inspected that the backup procedure includes information about backup frequency, backup location, and monitoring of failed backup jobs. We have inspected that the backup procedure is approved by management. We have, by sample test, inspected documentation for completed, successful backups.	No deviations noted.
3.5	Backup of information related to relevant systems and data is maintained and tested on a regular basis and in accordance with the procedure.	We have inspected that a formal procedure exists for periodic restore tests. We have, by sample test, inspected that restore tests carried out during the period have been completed successfully. We have inspected that, in the event of errors identified during restore tests, the error has been investigated and resolved, and the backup procedure has been adjusted if necessary.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 3 – Business continuity, such as back management, disaster recovery and crisis management

Formalised procedures and controls are in place to ensure continued operation and availability of services in case of disaster.

No.	*Bizbrains A/S' control activity*	*Grant Thorntons performed test*	*Test result*
3.6	The backup data is kept on a different location than the primary production site. Access and the logical connection between backup and production site is limited.	We have inspected that backups are stored at a physically separate location from the production environment. We have inspected that a segregation of duties has been established between backup and production data. We have inspected that the logical connection between backup and production locations is limited to predefined time windows.	No deviations noted.
3.7	The company has identified requirements for the availability of NIS2 related services and information systems through design and implementation of systems architecture with appropriate redundancy to meet these requirements.	We have inquired about the requirements for the availability of NIS2-related services. We have inspected that IT systems are designed with appropriate controls regarding redundancy to meet the availability requirements of NIS2 services.	No deviations noted.
3.8	The company has implemented controls ensuring sufficient redundancy to meet availability requirements, including availability of an alternate facility (i.e. disaster recovery site) not subject to the same threats as the primary facility, if relevant.	We have inquired about the availability of alternative facilities to continue operations in the event of major incidents or disasters where the primary facilities are unavailable. We have inspected that agreements have been made regarding alternative facilities in order to continue operations in the event of a crisis.	No deviations noted.
3.9	A crisis management plan based on risk assessment is implemented and approved by the management. The plan is maintained and includes procedures to ensure cybersecurity during crisis, defines roles and responsibility (incl. relevant service providers), communication channels and timelines tor authorities/CSIRT.	We have inspected the crisis management plan based on the risk assessment, which includes procedures to maintain cyber security during crises, defines roles and responsibilities (including relevant suppliers), as well as communication channels and timelines to authorities/CSIRT. We have inspected documentation confirming that the crisis management plan has been approved by management within the audit period.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 3 – Business continuity, such as back management, disaster recovery and crisis management

Formalised procedures and controls are in place to ensure continued operation and availability of services in case of disaster.

No.	*Bizbrains A/S' control activity*	*Grant Thorntons performed test*	*Test result*
3.10	The crisis management plan is tested and updated periodically (at least annually) and/or in case there are any changes. The result of the test is documented. Based on the result, relevant improvement/remediation initiatives are recorded and subsequently implemented	We have inspected documentation for the most recent test of the crisis management plan. We have inspected documentation confirming that the results of the crisis management plan test have been documented, and that relevant identified improvement measures have been recorded and subsequently implemented.	No deviations noted.
3.11	The company has implemented a process to manage and use information about for example security incidents, vulnerabilities, threats and measures that are obtained from the national CSIRT or where relevant the sector specific authorities.	We have inspected the handling of information such as security incidents, vulnerabilities, threats, and measures received from the national CSIRT or, where relevant, the sector-responsible authority.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 4 – Supply chain security, including security-related aspects concerning the relationships between the company and its direct suppliers or service providers

Formalised procedures and controls are in place to ensure relevant direct service providers (including suppliers) through the entire supply chain are identified and monitored to ensure compliance with company security requirements and service level

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
4.1	The company has implemented formalised procedures and processes to ensure the information security risk associated with the significant NIS2 related external service providers (for example power, technical assistance, Cloud vendors, OT, outsourced development etc.) is documented.	We have inspected that a formalised procedure has been designed and implemented to ensure a periodic assessment of information security risks in relation to NIS2-relevant external suppliers. We have inspected that the procedure is approved by management annually or when changes are made to the process. We have inspected that information security risks in relation to all NIS2-relevant external suppliers are evaluated and updated at least once a year.	No deviations noted.
4.2	The company has implemented a formalized procedure to ensure that significant NIS2 related external service providers and suppliers comply with the company's security requirements and measures.	We have inquired about the process of identifying and monitoring significant subcontractors. We have inspected that a formalised procedure has been developed and implemented to ensure that the company's security requirements are communicated to all significant external NIS2-related suppliers.	No deviations noted.
4.3	The company continuously monitors significant NIS2 related external service providers and suppliers for compliance with security measures, incident handling, significant changes etc.	We have, by sample test, inspected that the company has carried out monitoring of significant NIS2 subcontractors to ensure compliance with security requirements.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 4 – Supply chain security, including security-related aspects concerning the relationships between the company and its direct suppliers or service providers

Formalised procedures and controls are in place to ensure relevant direct service providers (including suppliers) through the entire supply chain are identified and monitored to ensure compliance with company security requirements and service level

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
4.4	Contracts with significant NIS2 related external service providers and suppliers include appropriate security requirements based on risks identified during risk assessment of the service provider.	We have inquired about the process for risk assessment of NIS2-relevant suppliers. We have inspected the risk assessment framework used, including that it contains requirements for assessment against relevant security requirements. For one sub-supplier, we have inspected that the company has carried out a risk assessment of NIS2-relevant suppliers for both technical and non-technical factors.	No deviations noted.
4.5	Mitigating actions are planned and implemented in a timely manner to address identified risks related to significant NIS2 related external service providers and suppliers.	We have inquired about the process for risk mitigation of NIS2-relevant suppliers. We have inspected that mitigating activities are planned and implemented for all NIS2-relevant suppliers.	No deviations noted.
4.6	Relevant assurance reports from significant NIS2 related external service providers and suppliers are subject to annual review. If substantial weaknesses are found, appropriate investigative actions are undertaken and mitigations for weaknesses put in place.	We have inspected that a formalised procedure exists to ensure that relevant assurance reports are obtained, and we have inspected this for NIS2-relevant service providers. We have, by sample test, inspected that relevant assurance reports have been obtained and reviewed for the NIS2-relevant supplier.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 5 – Security in network and information systems, acquisition, development, and maintenance, including vulnerability handling and disclosure

Formalised procedures and controls are in place to ensure that critical assets are properly developed, maintained and protected against vulnerabilities from internal and external threats.

No.	*Bizbrains A/S' control activity*	*Grant Thorntons performed test*	*Test results*
5.1	Network infrastructure and associated documentation is maintained and up-to-date. including network diagrams and configuration files of devices (e.g. routers, switches).	We have inspected that formalised documentation exists in the form of a network diagram as well as an overview of other relevant network equipment such as routers and switches. We have inspected documentation confirming that the network diagram and configuration are up to date.	No deviations noted.
5.2	The company has implemented a management approved procedure to ensure cybersecurity on the following areas: • When acquiring IT products or services from third parties • When developing and maintaining networks and information systems • When decommissioning/disposing of network and information systems The procedure is based on the company's information security policy, policy for risk management and policy for vendor management	We have inspected that the company has established an approved procedure to ensure cybersecurity in the following areas: • When acquiring IT products or services from third parties • When developing and maintaining networks and information systems • When decommissioning/disposing of networks and information systems We have inspected that the procedure is based on the company's information security policy as well as the policy for risk management and supplier management.	No deviations noted.
5.3	Lifecycle governance is continuously reviewed and updated at periodically or significant changes.	We have inspected documentation confirming that lifecycle governance is continuously reviewed and updated at predetermined intervals or upon significant changes.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 5 – Security in network and information systems, acquisition, development, and maintenance, including vulnerability handling and disclosure

Formalised procedures and controls are in place to ensure that critical assets are properly developed, maintained and protected against vulnerabilities from internal and external threats.

No.	*Bizbrains A/S' control activity*	*Grant Thorntons performed test*	*Test results*
5.4	Formalised procedures are implemented and regular assessments of the robustness of the systems and processes used by the company in the provision of NIS2 services are followed.	We have inspected that a formalised procedure exists for the ongoing assessment of the robustness of the company's systems and processes in relation to NIS2 services. We have inspected that the procedure has been updated and approved by management within the audit period.	No deviations noted.
5.5	The company has implemented a process for managing technical vulnerabilities and maintains capabilities/mechanisms to identify existing vulnerabilities in relation to NIS2 services.	We have inspected the procedure to ensure that relevant capacities/mechanisms are used to ensure that vulnerabilities have been assessed within the audit period.	No deviations noted.
5.6	Ongoing vulnerability scans are performed on assets used for NIS2 services.	We have inquired about the process for vulnerability assessment. We have inspected that scans of NIS2 services have been carried out, where vulnerabilities have been identified, risks assessed, prioritised, and resolved in a timely manner.	No deviations noted.
5.7	Network devices are hardened according to industry standard hardening configuration templates.	We have inspected that a baseline for hardening network devices exists, based on a recognised standard (such as CIS18). We have, by sample test, inspected that network devices are configured in accordance with the hardening baseline.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 5 – Security in network and information systems, acquisition, development, and maintenance, including vulnerability handling and disclosure

Formalised procedures and controls are in place to ensure that critical assets are properly developed, maintained and protected against vulnerabilities from internal and external threats.

No.	*Bizbrains A/S' control activity*	*Grant Thorntons performed test*	*Test results*
5.8	Internal networks have been segmented to ensure restricted access to systems and databases.	We have inquired about the practices and processes regarding network segmentation. We have inspected a network diagram showing that the internal network is segmented. We have inspected configuration files and rule sets in network devices that are intended to ensure effective network segmentation.	No deviations noted.
5.9	Changes to systems, databases or networks are made consistently with established procedures that ensure maintenance using relevant updates and patches, including security patches.	We have inspected that a formalised procedure exists describing the process for handling changes and patches. We have, by sample test, inspected that the implemented change and patch are managed and documented in accordance with the formalised procedure.	No deviations noted.

Control objective 6 – Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.

Formalised procedures and controls are in place to ensure that cyber related risk and threats are identified, monitored and remediated in timely manner.

No.	*Bizbrains A/S's control activity*	*Grant Thornton's performed test*	*Test result*
6.1	A management approved procedure is implemented to ensure that implemented security measures continue to be sufficient against relevant risks and internal requirements. The policy must assess whether the information security policy is in accordance with internal requirements, applicable legislation and relevant implementation acts (e.g. EU 2024/2690).	We have inspected that a management-approved procedure exists, which ensures that implemented security measures remain adequate in relation to relevant risks, internal requirements, applicable legislation, and relevant implementing acts. We have inspected documentation confirming that assessments of implemented security measures have been carried out.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 6 – Policies and procedures to assess the effectiveness of cybersecurity risk-management measures. Formalised procedures and controls are in place to ensure that cyber related risk and threats are identified, monitored and remediated in timely manner.			
No.	*Bizbrains A/S's control activity*	*Grant Thornton's performed test*	*Test result*
6.2	The procedure defines roles, methods and tools for performing assessments, including risk-based technical tests (e.g. scans and penetration tests). The procedure contains requirements for assessing compliance with legal/regulatory requirements, compliance with policies as well as the effectiveness and maintenance of the measures for the individual protected assets; it also includes the preservation of documentation and a remedial process for ineffective measures (owners, deadlines and follow-up).	We have inspected that the procedure defines roles, methods, and tools for carrying out assessments, including risk-based technical tests. We have inspected that the procedure includes requirements for assessing compliance with legal/regulatory requirements, adherence to policies, as well as the effectiveness and maintenance of measures for each protected asset, including the preservation of documentation and a process for following up on missing or ineffective measures.	No deviations noted.
6.3	The procedure is mapped to the company's information security policy, risk assessment and incident handling. The procedure is continuously reviewed and updated in case of major changes in the business and the threat picture.	We have inspected that the procedure has been developed based on the company's information security policy, risk assessment, and incident management. We have inspected that the procedure is reviewed and updated in the event of significant changes in the business and the threat landscape. We have inquired into whether there have been changes to the business or the threat landscape in the audit period.	We have been informed that there have been no significant changes to the business or the threat landscape during the audit period. No deviations noted.
6.4	In relation to critical infrastructure and applications, periodic tests are carried out based on a risk-based approach to test types (vulnerability scans, penetration tests, red/blue team activities, configuration reviews, code reviews, social engineering tests, testing of access controls), frequency, scope and triggering factors (installations, maintenance, upgrades, etc.). The test is documented, and irregularities are risk classified, followed for remediation and retested to confirm closure.	We have, by sample test, inspected that documented periodic testing of critical infrastructure and applications has been carried out, such as vulnerability scans, penetration tests, red/blue team activities, configuration reviews, code reviews, social engineering tests, and testing of access controls. We have inspected that irregularities are assessed, classified, and remediated.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 7– Basic cyber hygiene practices and cybersecurity training

Formalised procedures and controls are in place to ensure that cyber hygiene practices are implemented in the organisation, and employees complete ongoing training/education related to cyber security.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
7.1	Formalised procedures exist for cybersecurity awareness training, which include, but are not limited to the following: • Roles and entities included in management security training • Training of members of the management bodies • Knowledge sharing between members of management and essential and important entities of the company's organisation	We have inspected whether a formalised procedure exists for awareness training on cybersecurity, which includes, but is not limited to, the following: • Roles and responsibilities are clearly demonstrated in management/board training • Requirements for training and education of management/board members • Knowledge sharing and exchange between the company's management bodies We have inspected that the procedures are approved by management annually or when changes are made to the process.	No deviations noted.
7.2	Cyber hygiene policies and procedures are implemented, that includes but is not limited to the following: • establish a minimum set of baseline security policies (see "1. Risk analysis and security policy for information systems") • take regular backup copies of relevant data, test the backed-up data (integrity checks) and test procedures for recovery from backup (see "3. Backup") • plan capacity and resources (personnel and IT resources) to avoid potential capacity bottlenecks (see "3. Redundancy") • prepare a crisis management plan for incidents (see "3. Crisis management") • regularly evaluate the cyber security of the entity's IT supply chain (see "4. Supply chain security")	We have inquired about the process for monitoring the cyber hygiene programme. We have inspected that management has implemented monitoring controls to ensure compliance with cyber hygiene.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 7– Basic cyber hygiene practices and cybersecurity training

Formalised procedures and controls are in place to ensure that cyber hygiene practices are implemented in the organisation, and employees complete ongoing training/education related to cyber security.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
	• establish risk-based service level agreements (SLAs) with suppliers and service providers (see "4. Supply chain security") • regularly install patches and updates for operating systems and applications (see "5. Procurement, development and maintenance") • install and automatically update anti-malware software on all relevant assets (see "5. Procurement, development and maintenance") • segment the entity's network according to the criticality of the assets (see "5. Procurement, development and maintenance") • perform regular, automated vulnerability scans across the device's network and information systems (see "6. Technical tests") • carry out regular security tests (see "6. Technical tests") • build cyber security culture and awareness through regular user training (see "7. Cyber security training") • encrypt data at rest and in transit in accordance with asset classification levels (see "8. Cryptography") • limit administrative privileges (see "9. Access control") • enforce strong passwords (see "9. Access control") • apply multi-factor authentication (MFA) in accordance with asset classification levels (see "9. Access control") • limit network ports and services to what is strictly necessary for the entity's business needs (see "9. Access control") • maintain an inventory of hardware and software assets (see "9. Asset management")		

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 7– Basic cyber hygiene practices and cybersecurity training

Formalised procedures and controls are in place to ensure that cyber hygiene practices are implemented in the organisation, and employees complete ongoing training/education related to cyber security.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
7.3	Awareness training is provided to the company's management on a regular basis with respect to the NIS2 identified risks and control framework.	We have inquired about the process for awareness training of the company's management. We have inspected that awareness training has been conducted for the company's management in relation to NIS2-identified risks and control framework.	No deviations noted.
7.4	Awareness training is provided for the company's employees on a regular basis with respect to cybersecurity and general security awareness is covered in mandatory training.	We have inquired about the process for awareness training of the company's employees. We have inspected that employees' knowledge of cybersecurity has been tested.	No deviations noted.

Control objective 8 – Policies and procedures regarding the use of cryptography and, where appropriate, encryption.

Formalised procedures and controls are in place to ensure that critical assets are protected by encryption.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
8.1	Formalised procedures exist which include a requirement that effective encryption is applied to systems and hardware containing or transmitting NIS2 service data.	We have inspected that a formalised procedure has been designed and implemented to ensure the use of encryption in relation to systems and hardware, or the transfer of NIS2-relevant data. We have inspected that the procedure is approved by management annually or when changes are made to the process. We have, by sample test, inspected that encryption is used on systems and hardware that contain or transfer NIS2-relevant data.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 8 – Policies and procedures regarding the use of cryptography and, where appropriate, encryption. Formalised procedures and controls are in place to ensure that critical assets are protected by encryption.			
No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
8.2	Sensitive data used in delivering the NIS2 services is encrypted on End-User Devices.	We have inquired about the process for the use of encryption on end-user equipment. We have inspected the monitoring tool (e.g. management console) to validate that encryption of end-user devices is enabled. We have inspected that deviations are identified and remediated on an ongoing basis.	No deviations noted.
8.3	Cryptography solutions are used to safeguard where required and are formally approved and documented.	We have inquired about the process for the use of encryption. We have inspected that the implemented encryption solution is formally approved and documented. We have inspected that the approved encryption solution is implemented where required.	No deviations noted.
8.4	Strong cryptographic controls use non compromised versions of security protocols.	We have inspected that recognised cryptographic algorithms and protocols are used, and that they are updated to the latest version. We have inspected that the cryptographic algorithms used do not contain known vulnerabilities.	No deviations noted.
8.5	Cryptographic keys are managed tightly, in accordance with documented standards and procedures, and protected against unauthorised access or destruction.	We have inspected the procedure for handling cryptographic keys. We have inspected that cryptographic keys are protected against modification, loss, or unauthorised access/disclosure. We have inspected that systems used to generate, store, or archive keys are protected through the use of adequate access controls.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 8 – Policies and procedures regarding the use of cryptography and, where appropriate, encryption.

Formalised procedures and controls are in place to ensure that critical assets are protected by encryption.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
8.6	Effective encryption is applied when transmitting confidential/sensitive data through the internet or by email.	We have inquired about the process for the use of encryption when transferring confidential/sensitive data via the internet or email. We have inspected that encryption is used when transferring confidential and sensitive data via the internet and email.	No deviations noted.

Control objective 9 – Human resources security, access control policies and asset management.

Formalised procedures and controls are in place to ensure that human resources, access control and asset management are structured, formalised, and maintained to ensure an appropriate security level.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
9.1	A management-approved procedure is implemented ensuring that employees and – where relevant – suppliers/service providers are aware of and fulfil their responsibilities for the security of network- and information systems, in accordance with the company's information security policy. The procedure is reviewed and updated at planned intervals.	We have inspected the procedure to ensure that employees and suppliers/service providers are informed of and comply with their responsibilities for the security of networks and information systems in accordance with the entity's information security policy. We have inspected documentation confirming that the procedure has been reviewed and updated within the audit period.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 9 – Human resources security, access control policies and asset management.

Formalised procedures and controls are in place to ensure that human resources, access control and asset management are structured, formalised, and maintained to ensure an appropriate security level.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
9.2	The company has implemented and communicated employment (disciplinary) rules that apply in the event of violations of policies and procedures regarding the security of network- and information systems.	We have inspected documentation confirming that employment and disciplinary rules have been implemented and communicated, which apply in the event of violations of policies and procedures regarding the security of networks and information systems. We have, by sample test, inspected signed employment contracts for newly hired employees, in which the employees are informed about the employment and disciplinary rules that apply in the event of violations of policies and procedures regarding the security of networks and information systems.	No deviations noted.
9.3	The employees of the company are screened as part of the employment process. Such screening comprises, as relevant: • References from former employers • Criminal record • Diplomas	We have inspected the formalised procedure for screening new employees as part of the recruitment process. We have, by sample test, inspected that for employees hired during the audit period, screening has been carried out, including: • Obtaining references from previous employers • Criminal record certificate • Diplomas	No deviations noted.
9.4	Upon appointment, employees sign an employment contract and confidentiality agreement, where obligations for security responsibility are listed. The obligation will continue to remain valid upon resignation or dismissal.	We have inspected that a formalised procedure exists for obtaining confidentiality agreements. We have, by sample test, inspected that employees hired during the audit period have signed a confidentiality agreement, and that it also remains valid after the termination of employment.	No deviations noted.
9.5	Formalised procedures exist for access management including creating, maintaining and terminating access rights. In addition, the procedure includes requirements for segregation of duties in relevant areas.	We have inspected that a formal procedure exists for access management, including the granting, maintenance, and removal of access rights.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 9 – Human resources security, access control policies and asset management.

Formalised procedures and controls are in place to ensure that human resources, access control and asset management are structured, formalised, and maintained to ensure an appropriate security level.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
9.6	A formal process is in place ensuring that the allocation of access rights are based on a business justification - according to the "least privilege" principle.	We have inspected that a formal procedure exists for the granting of access rights, and that they are granted based on business need and according to the principle of least privilege. We have, by sample test, inspected that newly hired employees are granted access to systems based on the following parameters: • the granting of rights is approved in accordance with the procedure. • there is a business need for the access rights. • the rights are granted according to the principle of least privilege. • the granted rights are in accordance with the approved accesses.	No deviations noted.
9.7	The provision of passwords (secret authentication information) to users are controlled through a formal password management process.	We have inspected that the password configuration is in accordance with the password policy.	No deviations noted.
9.8	A formal process is in place ensuring that the removal of access rights is performed timely upon termination or changes of job functions.	We have inspected that a formal procedure exists for the timely removal of access rights upon termination of employment or change of job function. We have, by sample test, inspected that employees who have left the company during the audit period have had their access rights removed in a timely manner. We have, by sample test, inspected that employees with a change in job function in the audit period have had their access rights adjusted to the new job function.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 9 – Human resources security, access control policies and asset management.

Formalised procedures and controls are in place to ensure that human resources, access control and asset management are structured, formalised, and maintained to ensure an appropriate security level.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
9.9	A formal process is in place, ensuring that access rights are regularly reviewed.	We have inspected that a formalised procedure exists for periodic review of user access rights. We have inspected that a review of assigned user access rights has been carried out in accordance with the procedure within the audit period.	No deviations noted.
9.10	A formal process is in place, ensuring that system users and access to application functions are restricted in accordance with the access control policy.	We have inspected that a formalised procedure exists for system users and their access to application systems. We have, by sample test, inspected that system users' access to functions within applications is restricted in accordance with the access policy.	No deviations noted.
9.11	The allocation and use of privileged access rights is restricted and monitored. This also includes the use of supporting programs (Utility programs).	We have inspected that a formalised procedure exists for the use and monitoring of privileged access. We have inspected that privileged access is limited to individuals with a work-related need. We have inspected that privileged access is monitored.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 9 – Human resources security, access control policies and asset management.

Formalised procedures and controls are in place to ensure that human resources, access control and asset management are structured, formalised, and maintained to ensure an appropriate security level.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
9.12	The company has established a formalized process to create and maintain an overview of all relevant systems and processes for the delivery of NIS2 services. The following criteria are taken into account when identifying the scope of NIS2 service: Electronic communication network Any device or group of connected or related devices, one or more of which, by means of a program, performs automatic processing of digital data, or Digital data that is stored, processed, retrieved or transmitted by elements listed in the point above for the purpose of its operation, usage, protection and maintenance. The process is regularly assessed	We have inspected that the procedure for creating and maintaining an overview of relevant systems in relation to NIS2 services is formalised. We have inspected documentation confirming that an up-to-date overview of systems relevant to NIS2 services exists and is in accordance with applicable agreements.	No deviations noted.
9.15	Formalised procedures are in place to ensure disposal of media is only performed by qualified personnel and personnel have signed an NDA.	We have inspected that a formalised procedure exists for the secure disposal of media. We have, by sample test, inspected that disposed media have been securely disposed of by qualified personnel who have signed confidentiality agreements.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 9 – Human resources security, access control policies and asset management.

Formalised procedures and controls are in place to ensure that human resources, access control and asset management are structured, formalised, and maintained to ensure an appropriate security level.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
9.16	The company has implemented controls to minimise the risk of potential environmental threats e.g., fire, explosives, smoke, water, dust, chemical effects, electrical supply interference, communication interference, electromagnetic radiation.	We have inspected that a formalised procedure for physical and environmental security exists. We have inspected that the facilities are equipped with: • Burglar alarm • Fire and smoke alarm • Alarm for rising water • UPS and emergency power system We have inspected that the measures are subject to annual inspection.	No deviations noted.
9.17	The company keeps records of NIS2 relevant assets that are classified on the basis of significance to the customer, sensitivity and the need for confidentiality.	We have inspected the formalised procedure for handling information assets. We have inspected that the register of information assets and other related assets includes their classification.	No deviations noted.
9.18	Procedures are implemented that specify the secure termination of service providers (e.g. deactivation of access, ICT systems and deletion of associated data).	We have inspected the procedure for contract termination with NIS2-relevant suppliers. We have inspected that a formalised procedure exists to ensure the secure decommissioning/removal of NIS2-relevant assets and services. We have, by sample test, inspected that terminated employees in the audit period, related to NIS2 services, have had their assets securely decommissioned. We have inquired into whether there have been any decommissioned NIS2 services in the audit period.	We have been informed that there have been no decommissioned NIS2 services in the audit period. No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 10 – The use of multifactor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the company, where appropriate.

Formalised procedures and controls are in place to ensure a strong authentication process for access management to critical assets and secured emergency communication.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
10.1	Formalised procedures are in place defining requirements for utilising MFA (Multi Factor Authentication) or alternative continuous authentication solutions for communication systems within the company.	We have inspected that a formalised procedure has been designed and implemented to ensure requirements for the use of MFA (Multi-Factor Authentication) or other alternative solutions. We have inspected that the procedure has been approved by management within the audit period.	No deviations noted.
10.2	Access to high-risk networks and information systems are accessed as a minimum by using two-factor authentication for example when accessing: • Assets by remote access • Administrative systems • Sensitive information and confidential data Systems with high value to the company or with high consequences if compromised	We have inquired about the use of the two-factor authentication solution in the organisation. We have inspected that access to high-risk networks and information systems is, as a minimum, controlled via two-factor authentication.	No deviations noted.
10.3	Secure primary and secondary communication mechanisms are implemented supporting continued communication and reporting during a security incident.	We have inspected that a secure primary and secondary communication mechanism has been implemented to support continued communication and reporting in the event of a security incident. We have inspected that the use of the secondary communication channel is tested at least once a year.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

Control objective 10 – The use of multifactor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the company, where appropriate.

Formalised procedures and controls are in place to ensure a strong authentication process for access management to critical assets and secured emergency communication.

No.	*Bizbrains A/S' control activity*	*Grant Thornton's performed test*	*Test result*
10.4	Testing of secondary communication channels is performed on an annual basis.	We have inquired about the process for testing secondary communication channels. We have inspected that testing of secondary communication channels is carried out annually. We have inspected that the results of the test are evaluated and that mitigating actions are planned and initiated.	No deviations noted.

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

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

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

Mads Vigh
Underskriver 1
Serial number: 9e48e84c-fcc8-4da7-9673-58e68ad0c0d7
IP: 5.83.xxx.xxx
2026-11-05 08:58:32 UTC

Martin Brogaard Borup Nielsen
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serial number: 658bcd61-1988-4367-b3eb-215cfbbb49b0
IP: 104.28.xxx.xxx
2026-11-05 09:28:13 UTC

Kristian Randløv Lydolph
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
Serial number: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 62.243.xxx.xxx
2026-11-05 09:34:24 UTC

Penneo document key: D1HON-NAV3Y-IR58C-4Q9Z5-25LPV-D7R5Z

This document is digitally signed using **Penneo.com**. The signed data are validated by the computed hash value of the original document. All cryptographic evidence is embedded within this PDF for future validation.

The document is sealed with a Qualified Electronic Seal. For more information about Penneo's Qualified Trust Services, visit **https://eutl.penneo.com**.

How to verify the integrity of this document
When you open the document in Adobe Reader, you should see that the document is certified by **Penneo A/S**. This proves that the contents of the document have not been modified since the time of signing. Evidence of the individual signers' digital signatures is attached to the document.

You can verify the cryptographic evidence using the Penneo validator, **https://penneo.com/validator**, or other signature validation tools.