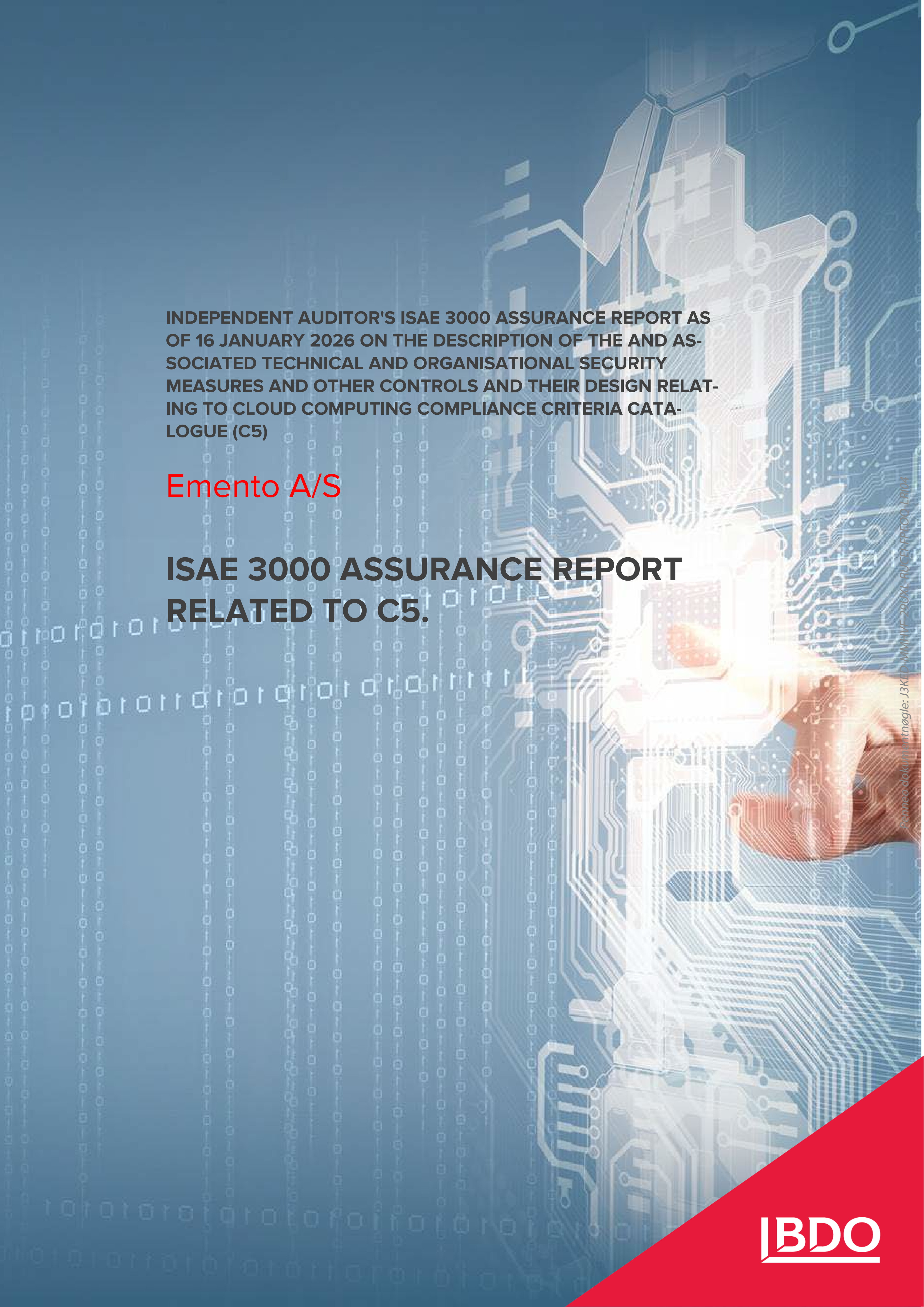

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT AS OF 16 JANUARY 2026 ON THE DESCRIPTION OF THE AND ASSOCIATED TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS AND THEIR DESIGN RELATING TO CLOUD COMPUTING COMPLIANCE CRITERIA CATALOGUE (C5)

Emento A/S

ISAE 3000 ASSURANCE REPORT RELATED TO C5.

INDHOLD

1. INDEPENDENT AUDITOR'S OPINION

INDEPENDENT AUDITOR'S ISAE 3000 REPORT AS OF 16 JANUARY 2026 ON THE DESCRIPTION OF THE EMENTO PRODUCT SUITE AND THE ASSOCIATED TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS AND THEIR DESIGN RELATING TO CLOUD COMPUTING COMPLIANCE CRITERIA CATALOGUE (C5)

To: The management of Emento A/S
Emento A/S Customers

Scope

We have been tasked with providing a declaration on the description prepared by Emento A/S (the cloud service provider) as of 16 January 2026 in section 3 of the Emento Product Suite and the associated technical and organisation security measures and other controls relating to C5.

We have not performed any procedures regarding the operational effectiveness of the controls included in the description and therefore express no conclusion on this.

Corporate Responsibility

The cloud service provider is responsible for preparing the statement in section 2 and the accompanying description, including the completeness, accuracy and the manner in which the statement and description is presented.

Furthermore, the cloud service provider is responsible for providing the services included in the description, as well as for stating the control objectives and designing and implementing controls to achieve the control objectives stated.

Auditor independence and quality management

We have complied with the requirements for independence and other ethical requirements of the International Ethics Standards Board of Auditors' International Guidelines on the Conduct of Auditors (IESBA Code), which are based on the fundamental principles of integrity, objectivity, professional competence and due diligence, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

BDO Statsautoriseret Revisionspartnerselskab applies International Standard on Quality Management 1 (ISQM 1) which requires that we design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legislation and other regulation.

Auditor's Responsibilities

Our responsibility is, on the basis of our procedures, to express an opinion on the cloud service provider’s description and on the design of controls related to the control objectives set out in this description.

We have performed our work in accordance with ISAE 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether the description is fairly presented, in all material respects, and whether the controls are appropriately designed, in all material respects.

An assurance engagement to provide a statement on the description and design of controls at a cloud service provider involves performing procedures to obtain evidence about the information in the cloud service provider 's description and the design of the controls. The actions chosen depend on our assessment, including the assessment of the risks that the description is not fair and that the controls are not appropriately 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 and described by the cloud service provider in section 2.

As described above, we have not performed procedures regarding the operating effectiveness of the controls included in the description and, accordingly, we do not express an opinion on this.

It is our opinion that the evidence obtained is sufficient and appropriate to provide a basis for our conclusion.

Limitations in controls

The cloud service provider's description is prepared to meet the common needs of a broad range of the cloud service provider's customers and therefore may not include every aspect of the use of the Emento Product Suite that each individual customer may consider important based on their specific circumstances. Furthermore, due to their nature, the cloud service provider's’s controls may not prevent or detect all errors or omissions.

Conclusion

Our conclusion is formed on the matters outlined in this report. The criteria we used in forming our conclusion are the criteria described in the cloud service provider's statement in section 2. It is our opinion that:

a. that the description of the Emento Product Suite and the associated technical and organisational security measures and other controls, as they were designed and implemented as of 16 January 2026 is fairly presented in all material respects, and

b. that the technical and organisational security measures and other controls related to the control objectives stated in the description were in all material respects suitably designed as of 16 January 2026.

Description of tests of controls

The specific controls that were tested and the results of these are detailed in section 4.

Intended users and purposes

This statement is intended only for the cloud service provider's customers who have used the cloud service provider's the Emento Product Suite and have sufficient understanding to consider it along with other information, including the technical and organisational security measures and other controls that the customers' own controls, when assessing the overall control environment.

Copenhagen, 3 February 2026

BDO Statsautoriseret Revisionspartnerselskab

Nicolai T. Visti Partner, State-Authorised Public Accountant	Mikkel Jon Larssen Partner, Head of Risk Assurance, CISA, CRISC

2. EMENTO A/S STATEMENT

The accompanying description is prepared for use of Emento A/S Customers who have used the Emento Product Suite and who have sufficient understanding to consider the description with other information, including the technical and organisational security measures and other controls that the customers themselves have implemented, when assessing the overall control environment.

Emento A/S use subcontractors. The relevant control objectives and related technical and organisational measures and other controls of the subcontractors are not included in the description.

Emento A/S confirms that the accompanying description in Section 3 provides a fair description of the Emento Product Suite and associated technical and organisational security measures and other controls of 16 January 2026. The criteria used to give this statement were that the accompanying description:

1. Explain the Emento Product Suite in relation to C5, and how the associated controls were designed and implemented, including explaining:
   - The procedures used to ensure that data processing has been carried out in accordance with C5.
   - The procedures that ensure that personnel authorized to process data have committed themselves to confidentiality or are subject to an appropriate duty of confidentiality.
   - Relevant control objectives and controls designed to achieve those objectives.
   - The controls that we would have designed and implemented with reference to the delineation of compliance with security requirements in relation to C5 and which, if necessary to achieve the control objectives, are identified in the description.
   - The controls that we have assumed, based on the scope of the Emento Product Suite, would have been designed and implemented by the customers and which, if necessary to achieve the control objectives, are identified in the description.
   - The other aspects of the control environment, risk assessment process, information systems and communications, control activities and monitoring controls relevant to the production of the services.
2. Does not omit or distort information relevant to the scope of the Emento Product Suite and the related controls considering that this description has been prepared to meet the general needs of a wide range of customers, therefore, it cannot include every aspect of the Emento Product Suite which the individual customer may consider of importance to their special environment.

Emento A/S confirms that the technical and organisational security measures and other controls associated with the control objectives stated in the accompanying description were suitably designed as of 16 January 2026. The criteria used to make this statement were that:

1. The risks that threatened the achievement of the control objectives set out in the description were identified.

2. The identified controls, if performed as described, would mitigate the relevant risks sufficiently to achieve the stated control objectives.

Aarhus N, 3 February 2026

Emento A/S

Allan Juhl
CEO

3. EMENTO A/S' DESCRIPTION OF THE EMENTO PRODUCT SUITE

This system description has been prepared to provide Emento A/S's customers with information about the requirements set out in C5 (Cloud Computing Compliance Criteria Catalogue). The controls have been developed based on Emento A/S's existing information security controls combined with the C5 criteria.

GENERAL DESCRIPTION OF EMENTO A/S

Emento A/S is a Danish-owned the cloud service provider developing, operating, maintaining and supporting the Emento Product Suite: Emento Patient Guide and _Guide.

The Emento Product Suite is a service for ongoing communication between user/patient/citizen and/or organisation/hospital/municipality. The platform consists of an app aimed at the citizen/patient and a web access aimed at the organisation's staff. The staff defines a process which guides and informs the citizen/patient continuously via an app.

Through the app, the citizen/patient can send messages to the unit, and the staff can respond when it suits. This reduces disruptive phone calls. Staff gain knowledge of the citizen/patient's interaction with the app and can use this to reduce unforeseen no-shows and cancellations.

To support the creation of good process guides and to ensure that learning can be quickly translated into new content or work processes, Emento A/S has developed a range of support products that enable staff to organise or adjust guides and content themselves.

Emento A/S hosts, operates, maintains, and supports the Emento Product Suite.

Emento A/S has approx. 23 employees who are specialised within system development, support, delivery, marketing, sales, finance, GDPR and information security. They are organised in a development and operations department, quality and support department, a delivery department and an administration department.

EMENTO PRODUCT SUITE AND PROCESSING OF CUSTOMER DATA

Emento A/S provides the Emento Product Suite, i.e. the Patient Guide and _Guide, as a Software-as-a-Service (SaaS) solution in accordance with concluded agreement with public authorities and private companies.

The Emento Product Suite is developed in Denmark and data is hosted within Hetzner's hosting data centres, which are located in Nuremberg, Germany and Helsinki, Finland. A data processor agreement has been made between Emento A/S and Hetzner.

The app can be used for several care/process guides from different customers. The citizen's profile is the same for all care guides. The data being processed includes full name, e-mail, profile image, telephone number, and identification, as well as in a few cases, confidential information, such as personal identification number and information about the type of course that the civilian may have.

A lighter version of the Emento Product Suite without MitID-validation and the possibility to immediately delete a citizen profile is sold under the brand_Guide. This solution is also hosted at Hetzner. This solution only contains a phone number and in some cases a profile image.

RISK MANAGEMENT OF THE EMENTO PRODUCT SUITE

An annual risk assessment is carried out and input for this assessment is obtained from all levels of the organisation.

Risk assessments are based on the implementation guidelines in the international standard ISO 27002 and 27005.

Emento A/S has a process to continuously identify, assess, and act on risks that may impact the business. All risks are assessed against well-defined criteria of likelihood and impact. This assessment, as well as the decision to respond, is documented in a risk analysis that reflects the reality of our business at all times.

Based on a risk assessment, the day-to-day Management of Emento A/S decides whether an identified risk can be accepted, is to be reduced or whether insurance is required, based on selected risks.

MANAGEMENT OF THE SECURITY OF IT AND CUSTOMER DATA

Emento A/S has prepared requirements for establishing, implementing, maintaining, and improving a management system for the security of customer data, which ensures compliance with the concluded agreements with the customer, and good data processor practice.

The technical and organisational security measures and other controls for protection of customer data are designed in accordance with the risk assessments and implemented to ensure confidentiality, integrity, and accessibility.

Management of the security of customer data and the technical and organisation security measures and other controls are structured in the following key areas, for which control objectives and control activities have been defined:

The table below presents the scope of the criteria included in this ISAE 3000 statement, together with a reference to the other information security frameworks applied by Emento A/S.

C5:2020 TITLE	REFERENCE	CONTROL AREA	GDPR Article	ISO 27001:2022	ISO 27001:2013 Annex A
1: Organisation of Information Security (OIS)	OIS01	Information security management system (ISMS)	5.2, 24, 32	4.1 - 10.2	
	OIS02	Guideline on information security	24, 32	6.2 A.5.1 A.5.2	A.5.1.1, A.5.1.2 A.6.1.1
	OIS03	Interfaces and dependencies	24, 32	4.3 -	
	OIS04	Segregation of duties		A.5.3 -	A.6.1.2
	OIS05	Contact with relevant authorities and interest groups		A.5.5 - A.5.6	A.6.1.3 A.6.1.4
	OIS06	Guideline for dealing with risks	32	6.1 8.2 8.3	A.7.1.1 A.9.2.3 A.9.4.1
	OIS07	Application of the procedure for dealing with risks	32	6.1 - 8.2 8.3	A.7.1.1 A.9.2.3 A.9.4.1
2: Security policies and work instructions (SP)	SP01	Documentation, communication and provision of policies and instructions	5.2, 24	A.5.1 -	A.5.1.1
	SP02	Review and approval of policies and instructions	5.2, 24	A.5.1 -	A.5.1.1
	SP03	Deviations from existing policies and instructions		N/A	

C5:2020 TITLE	REFERENCE	CONTROL AREA	GDPR Article	ISO 27001:2022	ISO 27001:2013 Annex A
3: Personnel (HR)	HR01	Verification of qualification and trustworthiness		A.6.1 -	A.7.1.1
	HR02	Employment and contractual conditions		A.6.2 -	A.7.1.2
	HR03	Safety training and awareness programme		A.6.3 -	A.7.2.2
	HR04	Regulatory process		A.6.4 -	A.7.2.3
	HR05	Responsibilities in the event of termination or change of employment		A.6.5	A.7.3.1
	HR06	Confidentiality agreements		A.6.2 - A.6.6	A.13.2.4 A.7.2.2
4: Asset Management (AM)	AM01	Inventory of the asset		A.5.9	A.8.1.1, A.8.1.2
	AM02	Guideline for the use and safe handling of assets	17	A.5.10 -	A.8.1.3, A.8.2.3
	AM03	Hardware commissioning		A.7.10 - A.8.9	A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5 NEW
	AM04	Decommissioning of assets	17	A.7.10 - A.8.10	A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5 NEW
	AM05	Obligation for authorised use and safe handling of assets handed out and return		A.5.11 - A.5.12	A.8.1.4 A.8.2.1
	AM06	Classification and labelling of assets	32	A.5.10 - A.5.12 A.5.13	A.8.1.3, A.8.2.3 A.8.2.1 A.8.2.2
5: Physical security (PS)	PS01	Security requirements for premises and buildings		N/A	
	PS02	Redundancy model		A.8.14 -	A.17.2.1
	PS03	Perimeter protection		A.7.1 A.7.2 A.7.3 A.7.4	A.11.1.1 A.11.1.2, A.11.1.6 A.11.1.3 NEW
	PS04	Access control		A.5.16 - A.5.18 A.7.2 A.7.3 A.7.4	A.9.2.1 A.9.2.2, A.9.2.5, A.9.2.6 A.11.1.2, A.11.1.6 A.11.1.3 NEW

C5:2020 TITLE	REFERENCE	CONTROL AREA	GDPR Article	ISO 27001:2022	ISO 27001:2013 Annex A
				A.8.2	A.9.2.3
	PS05	Protection against fire and smoke		A.7.3 - A.7.5	A.11.1.3 A.11.1.4
	PS06	Protection against failure of the supply systems		A.7.8 - A.7.11 A.7.12 A.7.13 A.8.14	A.11.2.1 A.11.2.2 A.11.2.3 A.11.2.4 A.17.2.1
	PS07	Monitoring of operating and environmental parameters		N/A	
6: Regular operation (OPS)	OPS01	Capacity management Planning		A.8.6	A.12.1.3
	OPS02	Capacity management monitoring		A.8.6 -	A.12.1.3
	OPS03	Capacity management control of resources		N/A	
	OPS04	Protection against malware concept		N/A	
	OPS05	Protection against malware implementation		A.8.7 -	A.12.2.1
	OPS06	Specifications for data backup and recovery concept		A.8.3 - A.8.10 A.8.13 A.8.24	A.9.4.1 NEW A.12.3.1 A.10.1.1, A.10.1.2
	OPS07	Data backup and restore Monitoring		N/A	
	OPS08	Data backup and restore Regular tests		A.8.13 -	A.12.3.1
	OPS09	Data backup and restore Storage		A.8.13 - A.8.14	A.12.3.1 A.17.2.1
	OPS10	Logging and monitoring concept		A.8.15	A.12.4.1, A.12.4.2, A.12.4.3
	OPS11	Logging and monitoring concept for handling metadata		A.8.10 - A.8.11 A.8.15	NEW NEW A.12.4.1, A.12.4.2, A.12.4.3
	OPS12	Logging and monitoring access, storage and deletion		A.8.3 - A.8.10 A.8.15	A.9.4.1 NEW A.12.4.1, A.12.4.2, A.12.4.3
	OPS13	Logging and monitoring Detection of events		A.5.25 A.8.16	A.16.1.4 NEW

C5:2020 TITLE	REFERENCE	CONTROL AREA	GDPR Article	ISO 27001:2022	ISO 27001:2013 Annex A
	OPS14	Logging and monitoring Retention of logging data		A.8.15 -	A.12.4.1, A.12.4.2, A.12.4.3
	OPS15	Logging and monitoring Attributability		N/A	
	OPS16	Logging and monitoring Configuration		A.8.9 - A.8.15 A.8.18	NEW A.12.4.1, A.12.4.2, A.12.4.3 A.9.4.4
	OPS17	Logging and monitoring Availability of the monitoring software		A.8.14 -	A.17.2.1
	OPS18	Dealing with weak points, faults and errors concept		A.8.8 -	A.12.6.1, A.18.2.3
	OPS19	Dealing with vulnerabilities, faults and errors		N/A	
	OPS20	Dealing with weak points, faults and errors Measurements, analyses and evaluation of processes		A.8.8 -	A.12.6.1, A.18.2.3
	OPS21	Involvement of the cloud customer in the event of incidents		A.8.8 -	A.12.6.1, A.18.2.3
	OPS22	Testing and documentation of open vulnerabilities		A.8.8 - A.8.32	A.12.6.1, A.18.2.3 A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
	OPS23	Dealing with weak points, faults and errors System hardening		A.8.9	NEW
	OPS24	Separation of data sets in the cloud infrastructure		A.8.22 -	A.13.1.3
7: Identity and access management (IDM)	IDM01	Policy for access and access authorisations	25, 32	A.5.15 - A.8.3 A.8.5	A.9.1.1, A.9.1.2 A.9.4.1 A.9.4.2
	IDM02	Assigning and changing access and access authorisations	25, 32	A.5.18 A.8.2	A.9.2.2, A.9.2.5, A.9.2.6 A.9.2.3
	IDM03	Blocking and revocation of access authorisations in the event of inactivity or multiple failed logins		A.5.18 -	A.9.2.2, A.9.2.5, A.9.2.6
	IDM04	Withdrawal or adjustment of access authorisations if the area of responsibility changes	25, 32	A.5.18 - A.8.2	A.9.2.2, A.9.2.5, A.9.2.6 A.9.2.3

C5:2020 TITLE	REFERENCE	CONTROL AREA	GDPR Article	ISO 27001:2022	ISO 27001:2013 Annex A
	IDM05	Regular review of access authorisations	25, 32	A.5.18 -	A.9.2.2, A.9.2.5, A.9.2.6
	IDM06	Privileged access authorisations		A.5.3 - A.8.2 A.8.15 A.8.16	A.6.1.2 A.9.2.3 A.12.4.1, A.12.4.2, A.12.4.3 NEW
	IDM07	Access to cloud customer data	28, 32	N/A	
	IDM08	Confidentiality of authentication information		A.5.17 -	A.9.2.4, A.9.3.1, A.9.4.3
	IDM09	Authentication mechanisms		A.5.17 -	A.9.2.4, A.9.3.1, A.9.4.3
8: Cryptography and key management (CRY)	CRY01	Policy on the use of encryption methods and key management	32	A.5.14 A.5.31 A.8.24	A.13.2.1, A.13.2.2, A.13.2.3 A.18.1.1, A.18.1.5 A.10.1.1, A.10.1.2
	CRY02	Encryption of data during transmission (transport encryption)	32	A.5.14 A.5.31 A.8.20 A.8.24 A.8.26	A.13.2.1, A.13.2.2, A.13.2.3 A.18.1.1, A.18.1.5 A.13.1.1 A.10.1.1, A.10.1.2 A.14.1.2, A.14.1.3
	CRY03	Encryption of sensitive data during storage	32	A.5.34 A.8.24	A.18.1.4 A.10.1.1, A.10.1.2
	CRY04	Secure key management		A.8.24 -	A.10.1.1, A.10.1.2
9: Communication security (COS)	COS01	Technical protective measures		A.8.12 - A.8.20 A.8.21	NEW A.13.1.1 A.13.1.2
	COS02	Security requirements for connections in the cloud service provider's network		A.5.14 - A.8.20	A.13.2.1, A.13.2.2, A.13.2.3

C5:2020 TITLE	REFERENCE	CONTROL AREA	GDPR Article	ISO 27001:2022	ISO 27001:2013 Annex A
				A.8.21 A.8.22	A.13.1.1 A.13.1.2 A.13.1.3
	COS03	Monitoring of connections in the cloud service provider's network		A.5.14 A.8.9 A.8.16 A.8.20 A.8.21	A.13.2.1, A.13.2.2, A.13.2.3 NEW NEW A.13.1.1 A.13.1.2
	COS04	Crossnetwork access		A.8.21 - A.8.22	A.13.1.2 A.13.1.3
	COS05	Networks for administration		A.8.22 -	A.13.1.3
	COS06	Segregation of data traffic in shared network environments		A.8.22 -	A.13.1.3
	COS07	Documentation of the network		A.8.9 -	NEW
	COS08	Data transmission policy		A.5.14 A.8.12	A.13.2.1, A.13.2.2, A.13.2.3 NEW
10: Portability and interoperability (PI)	PI01	Documentation and safety of the input and output interfaces	28	A.8.9 -	NEW
	PI02	Contractual agreements for the provision of data		N/A	
	PI03	Secure data erasure	17	A.7.14	A.11.2.7
11: Procurement, development and modification of information systems (DEV)	DEV01	Guidelines for the development / procurement of information systems		A.5.8 A.8.25 A.8.26 A.8.27 A.8.28 A.8.31	A.6.1.5, A.14.1.1 A.14.2.1 A.14.1.2, A.14.1.3 A.14.2.5 NEW A.12.1.4, A.14.2.6
	DEV03	Guidelines for the modification of information systems		8.1 - A.8.32	A.11.2.8 A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
	DEV04	Security training and awareness programme for continuous software		7.2 A.6.3 A.8.32	A.11.1.6 A.7.2.2

C5:2020 TITLE	REFERENCE	CONTROL AREA	GDPR Article	ISO 27001:2022	ISO 27001:2013 Annex A
		deployment and associated systems, components or tools			A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
	DEV05	Risk assessment, categorisation and prioritisation of changes		8.1 - A.8.32	A.11.2.8 A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
	DEV06	Testing the changes		A.8.29 - A.8.32	A.14.2.8, A.14.2.9 A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
	DEV07	Logging of changes		A.8.4 - A.8.29 A.8.32	A.9.4.5 A.14.2.8, A.14.2.9 A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
	DEV08	Version control		7.5.3 A.8.32	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
	DEV09	Approvals for deployment in the production environment		A.8.32	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
	DEV10	Separation of the environments		A.8.11 - A.8.31	NEW A.12.1.4, A.14.2.6
12: Control and monitoring of service providers and suppliers (SSO)	SSO01	Guidelines and instructions for controlling and monitoring third parties		A.5.19 - A.5.20 A.5.21 A.6.3	A.15.1.1 A.15.1.2 A.15.1.3 A.7.2.2
	SSO02	Risk assessment of service providers and suppliers		A.5.19 - A.5.20 A.5.21	A.15.1.1 A.15.1.2 A.15.1.3
	SSO03	List of service providers and suppliers		N/A	
	SSO04	Monitoring compliance with the requirements		A.5.22 -	A.15.2.1, A.15.2.2

C5:2020 TITLE	REFERENCE	CONTROL AREA	GDPR Article	ISO 27001:2022	ISO 27001:2013 Annex A
	SSO05	Exit strategy for the receipt of benefits		A.5.23 -	NEW
13: Security incident management (SIM)	SIM01	Guideline for dealing with security incidents	33, 34	A.5.24 - A.5.25 A.5.26 A.5.27 A.6.8	A.16.1.1 A.16.1.4 A.16.1.5 A.16.1.6 A.16.1.2, A.16.1.3
	SIM02	Processing of security incidents	33, 34	A.5.5 + A.5.6 A.5.7 A.5.24 A.5.25	A.6.1.3 A.6.1.4 NEW A.16.1.1 A.16.1.4
	SIM03	Documentation and reporting of security incidents	33, 34	A.5.24 - A.5.28	A.16.1.1 A.16.1.7
	SIM04	Obligation for users to report security incidents to a central office		A.6.8 -	A.16.1.2, A.16.1.3
	SIM05	Evaluation and learning process		A.5.7 + A.5.25 A.5.26 A.5.27 A.6.8	NEW A.16.1.4 A.16.1.5 A.16.1.6 A.16.1.2, A.16.1.3
14: Business continuity and contingency management (BCM)	BCM01	Responsibility of the cloud service provider management		A.5.29 - A.5.30	A.17.1.1, A.17.1.2, A.17.1.3 NEW
	BCM-02	Guidelines and procedures for business impact analysis		A.5.29 - A.5.30	A.17.1.1, A.17.1.2, A.17.1.3 NEW
	BCM-03	Business continuity planning		A.5.29 - A.5.30	A.17.1.1, A.17.1.2, A.17.1.3 NEW
	BCM-04	Verification, updating and testing of business continuity		A.5.29 - A.5.30	A.17.1.1, A.17.1.2, A.17.1.3 NEW
15: Compliance (COM)	COM01	Identification of applicable legal, regulatory, selfimposed or contractual requirements		A.5.31	A.18.1.1, A.18.1.5
	COM-02	Guideline for planning and conducting audits		9.2 - A.8.34	A.12.7.1

C5:2020 TITLE	REFERENCE	CONTROL AREA	GDPR Article	ISO 27001:2022	ISO 27001:2013 Annex A
	COM-03	Internal audits of the information security management system		9.2 9.3 A.5.36 A.8.34	A.18.2.2, A.18.2.3 A.12.7.1
	COM-04	Information on the information security performance and management assessment of the ISMS		9.3	
16: Dealing with investigations from government agencies (INQ)	INQ01	Legal assessment of investigation enquiries	15, 48	N/A	
	INQ02	Informing customers about investigation requests	15, 48	N/A	
	INQ03	Requirements for accessing or disclosing data in response to investigation requests	15, 48	N/A	
	INQ04	Limitation of access to or disclosure of data in the event of investigation requests	15, 48	N/A	
17: Product safety and security (PSS)	PSS01	Guidelines and recommendations for customers		N/A	
	PSS02	Identification of vulnerabilities of the cloud service		A.8.8 -	A.12.6.1, A.18.2.3
	PSS03	Online register of known vulnerabilities		N/A	
	PSS04	Error handling and logging mechanism		N/A	
	PSS05	Authentication mechanisms		N/A	
	PSS06	Session Management		N/A	
	PSS07	Confidentiality of authentication information		N/A	
	PSS08	Roles and rights concept		A.5.15 - A.8.3 A.8.5	A.9.1.1, A.9.1.2 A.9.4.1 A.9.4.2
	PSS09	Authorisation mechanisms		A.5.15 - A.8.3 A.8.5	A.9.1.1, A.9.1.2 A.9.4.1 A.9.4.2
	PSS12	Locations of data processing and storage	Chapter V (44-50)	N/A	

C5 CONTROL AREA FRAMEWORK AND CRITERIA FOR CONTROL IMPLEMENTATION

Emento A/S wishes to maintain and continuously develop a level of IT security in line with the requirements outlined in the C5 and the ISO 27001 - Information Security. The requirements are tightened in well-defined areas where there are special legal requirements, contractual conditions or possibly special risk (identified by a risk assessment).

An effective defense against IT security threats must be created in order to best safeguard Emento A/S's image and the security and working conditions of its employees. The protection must address natural as well as technical and man-made threats. All persons are considered to be a possible cause of a security breach, i.e. no group of people should be above the security rules.

The objectives are therefore to ensure:

- AVAILABILITY - by achieving high reliability with high uptime percentages and minimised risk of major outages and data loss.
- INTEGRITY - by achieving correct functioning of the systems with minimised risk of manipulation and errors in both data and systems.
- CONFIDENTIALITY – by achieving confidentiality in the processing, transmission and storage of data.
- AUTHENTICITY - by achieving mutual security around the parties involved.
- INDEPENDENCE - by obtaining a guarantee of mutual and documentable contact.

The following control areas in The Cloud Computing Compliance Criteria Catalogue C5:2020 were assessed:

OIS: Organisation of Information Security

Emento A/S has established a formal framework for managing information security, with the cloud service provider's CEO holding the formal responsibility for IT security and the approval of the information security policy and guidelines on information security including guideline for dealing with risks. Management actively participates in security matters, supported by an organisational security and data protection committee with members from all relevant departments to coordinate activities. Security responsibilities are clearly defined within the security policy.

SP: Security Policies and Instructions

Emento A/S maintains a formal information security policy, which is documented and distributed in an information security handbook. This policy framework includes specific instructions for the daily management of information and data. All employees receive the policy upon hiring and are required to stay updated on its contents and related procedures. Policies and handbooks are formally reviewed and approved annually, or whenever significant changes occur. The policy is also reassessed annually by Management to ensure its continued relevance and effectiveness. Furthermore, key suppliers and business partners are made familiar with the information security policy.

HR: Personnel

Emento A/S has implemented controls covering the entire employment lifecycle to ensure that personnel are qualified and aware of their security responsibilities. Before employment, applicants must provide an unblemished criminal record. Upon joining, employees contractually commit to comply with the cloud service providers policies, including the security policy. Emento A/S fosters continuous security awareness through ongoing training and communication of policy changes at staff meetings and committee meetings. Confidentiality obligations are integral to all employment contracts. A formal departure process ensures that upon termination of employment, all access rights are revoked, and the cloud service provider equipment is returned, with the immediate manager and CEO holding responsibility for this process. Breaches of the security policy are subject to sanctions, which are handled by management on a case-by-case basis.

AM: Asset Management

Emento A/S has implemented controls to ensure the appropriate protection of its equipment and data assets. All relevant equipment is registered in a service desk system, which also tracks all changes. A centrally updated list of all authorized mobile devices is also maintained. The use of IT equipment by employees is governed by fixed guidelines defined in the information security handbook. All data processing activities must adhere to the guidelines outlined in the information handling policy, which includes sanctions for non-compliance.

PS: Physical Security

Emento A/S ensures that IT equipment is protected from unauthorized physical access and environmental threats. Physical access to Emento A/S's premises is restricted to authorized personnel via personal key rings, and any external parties must be escorted. For its hosting environments, Emento A/S utilizes the data centers of Hetzner. The physical and environmental security of these data centers, including access controls, is the responsibility of these providers. Emento A/S relies on certifications from Hetzner to ensure their controls are effective.

OPS: Operations

Emento A/S ensures that the operation of its servers and key systems is performed in a structured and secure manner. Documented operating procedures are available and enforced through automation via dev-ops scripts and platforms. Capacity is systematically monitored across the infrastructure to plan for future needs. Data is backed up according to customer agreements, with failed backups being logged and monitored. General backup tests are performed annually. To protect against malware, all servers are automatically patched and updated, and workstations are equipped with antivirus software. Emento A/S employs extensive logging and monitoring, with all incidents registered in an IT Service Management System and critical alarms displayed continuously to be addressed by the relevant personnel. Emento A/S continuously obtains information about technical vulnerabilities.

IDM: Identity and Access Management

Emento A/S has implemented robust controls to ensure access to systems and data is granted based on a work-related need and is revoked when no longer necessary. A formal policy and procedure for access management governs the process. User rights are allocated based on the principle of least privilege, determined by the employee's role and function. The creation and deletion of user accounts are tied to formal HR employment checklists. The security and data protection committee periodically reviews all user access and rights. Strong password rules are enforced using 1Password, and separate administrative profiles are used for all operational staff where technically possible.

CRY: Cryptography and Key Management

Emento A/S has implemented controls to ensure the correct and effective use of cryptography to protect the confidentiality, authenticity, and integrity of data. All data exchanges are subject to encryption. External communications containing sensitive personal information are encrypted in transmission using technologies like TLS. Databases containing personal data and their corresponding backups are encrypted. Furthermore, data stored on personal devices is encrypted to prevent unauthorized access. Recovery keys and certificates are stored securely, and the algorithms and encryption levels used are risk-assessed on an ongoing basis to align with the current threat level.

COS: Communication Security

Emento A/S has implemented controls to ensure its infrastructure components are operated securely. The network is protected by centrally managed firewalls that control all traffic based on defined rules, with all incoming traffic being logged. Written procedures exist for the configuration of firewalls, routers, and switches, which are handled exclusively by the operations department. Customer networks are logically separated and limited using VLANs and access rules in the core router/firewall, ensuring that only approved Emento A/S personnel can access different customer VLANs. The network is segmented into several virtual networks (VLANs) to control traffic flow between them.

PI: Portability and Interoperability

Emento A/S has established policies and procedures to ensure that upon termination of a contract, personal data is either returned to the controller or securely deleted in accordance with the controller's instructions.

This commitment ensures that customers can manage their data at the end of the service relationship, supporting data portability and the right to erasure.

DEV: Procurement, Development and Modification of Information Systems

Emento A/S has implemented controls to ensure systems are developed, acquired, and maintained in a structured and secure process. A formal Change Management procedure, with workflows managed in a service desk system, governs all major changes to ensure they are properly reassessed and tested. Emento A/S's development process adheres to the principles of data protection by design and by default. Development, testing, and production environments are kept separate, and anonymized data is used for testing purposes. Security patches for systems are installed automatically, while other updates are deployed with new releases of the Emento product Suite. A version control system is in use, which makes it possible to reinstall previous versions if required.

SSO: Control and Monitoring of Service Providers and Suppliers

Emento A/S use subcontractors. Emento A/S manages these relationships through a defined control framework. For any subcontractors whose services are an integral part of Emento A/S 's offerings, Emento A/S inspects their controls by obtaining and reviewing auditor reports such as ISAE 3402 or similar documentation. These subcontractors are assessed before an agreement is entered into and are monitored annually based on a risk assessment. Emento A/S ensures that any subcontractors are bound by the same protection obligations as Emento A/S through data processing agreements, and their use requires prior written approval from the customer.

SIM: Security Incident Management

Emento A/S has established controls to ensure security incidents are managed in a timely and effective manner. All incidents are handled according to a formal Incident Management procedure and are registered in Emento A/S's IT Service Management System. The process includes Problem Management to identify the root cause of incidents and to implement preventive and corrective measures.

BCM: Business Continuity Management

Emento A/S maintains a formal contingency plan which is updated as required and tested annually to ensure its effectiveness. The plan, which incorporates information security, defines roles and responsibilities and is designed to restore operations and ensure access to data within an acceptable timeframe following an outage. The contingency plan is reviewed and updated at least once a year in conjunction with management's review of the security policy and risk assessments. Detailed plans for system and data re-establishment are documented, and a copy is stored securely at an off-site location.

COM: Compliance

Emento A/S ensures compliance with legal, contractual, and internal policy requirements through a structured framework. The cloud service provider maintains an overview of applicable laws and requirements, with a written procedure for identifying new compliance obligations. All customer and supplier contracts, including Data Processing Agreements (DPAs), are reviewed and managed to ensure compliance. Compliance with data processor and supplier contracts is monitored on a regular basis. The cloud service provider performs regular reviews of their policies and conducts internal audits annually.

INQ: Dealing with investigation requests from government agencies

Emento A/S has established procedures to ensure that any investigation requests from government agencies are handled in an appropriate and lawful manner. These procedures include a legal assessment to verify the validity of each request. Emento A/S's policy is to inform affected customers of such requests unless legally prohibited from doing so. Access to or disclosure of customer data in response to a request is strictly limited to the data that is legally required to be disclosed, ensuring that the scope is not unnecessarily broad.

PSS: Product Safety and Security

Emento A/S provides its Product Suite with a range of security features and ensures customers have the necessary information and controls to use the service securely. User access to the Emento Product Suite is secured with strong authentication through MitID validation. Customers are responsible for their use of the platform and are provided with the means to control user privileges, including the allocation of administrator rights within their own environment. Emento A/S manages technical vulnerabilities in the underlying platform through regular scanning and an automated patching process. Emento A/S has implemented procedures for assisting the Controller in complying with their obligations regarding data subjects' rights and providing all necessary information to demonstrate compliance.

COMPLEMENTARY CONTROLS AT THE CLOUD SERVICE PROVIDER

The customer is obligated to implement the following technical and organisational security measures and other controls to achieve the control objectives and thereby comply with relevant legislation:

- The customer is responsible for ensuring that the administrators’ use of The Emento Product Suite is in accordance with relevant legislation.
- The customer controls the user privileges in The Emento Product Suite, including to whom administrator access is allocated and which rights are granted to the individual administrators.

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND TEST RESULTS

Purpose and scope

We conducted our engagement in accordance with ISAE 3000, Assurance Reports Other Than Audits or Reviews of Historical Financial Information.

BDO has performed procedures to obtain evidence of the information of Emento A/S ’s description of the Emento Product Suite and of the design of these relating controls. The selected procedures depend on BDO’s assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed.

BDO’s test of the design of controls and the implementation hereof have included the control objectives and related control activities selected by Emento A/S, and which are described in the following control form.

In the control form, BDO has described the tests performed and considered necessary to obtain reasonable assurance about whether the stated control objectives were achieved and whether the related controls were suitably designed as of 16 January 2026.

Performed test actions

Tests of the design of controls and the implementation hereof were performed by inquiry, inspection and observation.

Type	Beskrivelse
Inquiry	Inquiries of relevant personnel have been performed for all significant control activities. The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e., whether the design of the controls is expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission, and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.

For the services provided by Hetzner Online GmbH within hosting, we have received an ISO 27001 certification for the period 27 September 2019 to 26 September 2025, and an internal safety report signed in 2025 on technical and organisational security measures relating to operation of the hosting services.

For the services provided by OnlineCity A/S within SMS gateway (GatewayAPI), we have received from an independent auditor the ISAE 3402 report for the period 1 May 2024 to 30 April 2025 on technical and organisational security measures relating to operation of the SMS gateway.

For the services provided by Rambøll within SurveyXact, we have received from an independent auditor the ISO 27001 Certificate for the period 26 June 2024 to 25 June 2027 and the ISAE 3000 report for the period 1 June 2024 to 30 April 2025 on technical and organisational security measures relating to operation in SurveyXact.

For the services provided by Kontainer A/S within digital asset management, we have received from an independent auditor the ISAE 3402 report for the period 1 April 2024 to 31 May 2025 on technical and organisational security measures relating to operation of Digital Asset Management.

For the services provided by TwentyThree within Video platforms, we have received from an independent auditor the ISAE 3000 assurance report on information security and measures for the period from 1 February 2024 to 31 July 2025 on technical and organisational security measures relating to operation of the video platform.

With respect to the services provided by Meedio within video conferencing, we have from an independent auditor received the TÜV Certificate for the period 15 December 2023 to 15 December 2026 as well as the ISAE 3000 GDPR report for the period 1 September 2022 to 29 February 2024 on technical and organisational security measures relating to operation of the video conferencing.

This subcontractor's relevant control objectives and related controls are not included in Emento A/S's description of Emento Product Suite and the related controls. Accordingly, we have only inspected the documentation received and tested the controls at Emento A/S, which ensure monitoring of the subcontractor's fulfilment of the agreement entered between the subcontractor's and Emento A/S.

Result of test

The result of the tests performed indicates whether the described test has given rise to note exceptions.

An exception exists when:

1. Controls have yet to be designed or implemented to fulfil a control objective.
2. Controls related to a control objective are not suitably designed or implemented.

Organisation of Information Security (OIS)

Objective

- *Plan, implement, maintain and continuously improve the information security framework within the organisation*

Control activity	Test performed by BDO	Result of test
OIS-01 - Information security management system (ISMS) ▶ The cloud service provider operates an information security management system (ISMS) in accordance with ISO/IEC 27001. The scope of the ISMS covers the cloud service provider's organisational units, locations and procedures for providing the cloud service. ▶ The cloud service provider has implemented an information security policy.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider has an established ISMS in accordance with ISO 27001. We have inspected the scope of the ISMS covers the cloud service provider's organisational unit, location and procedures for providing the cloud service. We have inspected that the cloud service provider's SoA. We have inspected the latest management review and observed that the cloud service provider has reviewed and approved the information security management system (ISMS). We have inspected the cloud service provider's information security policy and observed that it has been approved by the CEO on august 12th 2025.	No deviations were found.
OIS-02 - Guideline on information security ▶ The top management of the cloud service provider has adopted guidelines on information security and communicated it to internal and external employees as well as cloud customers.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider has an information security policy with underlying guidelines. We have inspected the cloud service provider's information security policy and observed that it has been approved by the CEO on august 12th 2025. We have inspected relevant guidelines and found that they have been communicated to internal employees. We have by sample inspected that the information security policy and the underlying guidelines have been signed by employees.	No deviations were found.

Organisation of Information Security (OIS)

Objective

- *Plan, implement, maintain and continuously improve the information security framework within the organisation*

Control activity	Test performed by BDO	Result of test
	By inquiry we have been informed that the cloud service provider has no external employees.	
OIS-03 - Interfaces and dependencies - Interfaces and dependencies between activities for providing the cloud service that are carried out by the cloud service provider itself and activities that are carried out by third parties are documented and communicated. - This includes the handling of the following events: ○ Vulnerabilities ○ Security incidents and ○ Malfunctions - Changes to the interfaces and dependencies are communicated in such a timely manner that the affected third parties can respond appropriately with organisational and technical measures before they take effect.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider has written interfaces in their Information security description. We have inspected, that the description includes vulnerabilities, security incidents and malfunctions. By inquiry we have been informed that no changes have been made since the introduction of the procedure.	We have found that no changes have been made since the introduction of the procedure. We have therefore not been able to test the implementation of the control. No deviations were found.
OIS-04 - Segregation of duties - The cloud service provider has a clearly divided organisation in relation to information security and has detailed descriptions of responsibilities and roles for the individual employees. - The conflicting functions and responsibilities of the cloud service provider are separated, to the extent possible, considering the size of the cloud service provider, to reduce the possibility of unauthorised or unintentional use, alteration or misuse of data.	We have conducted inquiries with appropriate personnel at the cloud service provider. We inspected the cloud service provider's IT security handbook includes organisational and technical segregation of duties. By inquiry we have been informed, segregation of duties is enforced by management approval on all user creations. We have by a random sample inspected that access rights are approved by management. We have by random inspection, observed that conflicting functions and responsibilities of the cloud service provider are separated.	No deviations were found.

Organisation of Information Security (OIS)

Objective

- *Plan, implement, maintain and continuously improve the information security framework within the organisation*

Control activity	Test performed by BDO	Result of test
OIS-05 - Contact with relevant authorities and interest groups ▶ The cloud service provider keeps up to date with news from authorities	We have conducted inquiries with appropriate personnel at the cloud service provider. We have by random sample inspected that the cloud service provider continuously keep itself up to date through newsletters from authorities.	No deviations were found.
OIS-06 - Guideline for dealing with risks ▶ The cloud service provider has established a risk assessment procedure including: ○ Identification of risks related to the loss of confidentiality, integrity, availability and authenticity of information, ○ Analysing the probability of occurrence and impact in the event of occurrence and determining the risk level, ○ Evaluation of the risk analysis ○ Treatment of risks through measures. ○ Documentation of the activities for applying the procedure in order to obtain consistent, valid and comparable results in the event of repeated application.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the risk assessment procedure and observed that the cloud service provider continuously updates risk assessments based on ISO 27005. We have inspected the risk assessment and observed that it includes the loss of confidentiality, integrity, availability and authenticity of information. We have inspected that the risk assessment is updated in TRUST meetings and is approved by management.	No deviations were found.
OIS-07 - Application of the procedure for dealing with risks ▶ The cloud service provider shall apply the procedure for dealing with risks on an ad hoc basis, but at least annually.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the risk assessment is evaluated and updated continuously.	No deviations were found.

Safety guidelines and work instructions (SP)

Objective

- *Provide policies and instructions regarding security requirements and to support business requirements.*

Control activity	Test performed by BDO	Result of test
SP-01 - Documentation, communication and provision of guidelines and instructions ▶ Guidelines and instructions derived from the information security policy are documented according to a standardised structure. They are communicated and made available to all internal and external employees of the cloud service provider in an appropriate and needs-based manner. ▶ The guidelines and instructions are versioned and approved by the cloud service provider's top management or authorised personnel.	We have conducted inquiries with appropriate personnel at the cloud service provider. By inquiry we have been informed that guidelines and instructions derived from the information security policy are documented according to a standardised structure. We have inspected by random samples that the procedures are according to a standardised structure. We have inspected by random sample, that procedures are approved by top management. We have inspected that procedures are communicated to relevant employees.	No deviations were found.
SP-02 - Review and approval of guidelines and instructions ▶ The information security guidelines and instructions are reviewed at least once a year by expert personnel of the cloud service provider to ensure that they are appropriate.	We have conducted inquiries with appropriate personnel at the cloud service provider. By inquiry we have been informed that all procedures must be reviewed at least once a year. We have inspected documentation on periodic review. We have randomly inspected, that procedures are reviewed and approved at least once a year.	No deviations were found.
SP-03 - Deviations from existing guidelines and instructions ▶ Exceptions to information security policies and instructions go through the risk management process, including approval of the exceptions and acceptance of the associated risks by the risk owners.	We have conducted inquiries with appropriate personnel at the cloud service provider.	We have noted that the cloud service provider does not deviate from their policies or procedures. We have therefore not been able to test the implementation of this part of the control.

Safety guidelines and work instructions (SP)		
Objective ▶ *Provide policies and instructions regarding security requirements and to support business requirements.*		
Control activity	**Test performed by BDO**	**Result of test**
	By inquiry we have been informed that all exceptions to policies and procedures need approval and will be incorporated in the risk assessment. By inquiry we have been informed that the cloud service provider doesn't deviate from their policies or procedures.	No deviations were found.

Personnel (HR)		
Objective ▶ *Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.*		
Control activity	**Test performed by BDO**	**Result of test**
HR-01 - Verification of qualification and trustworthiness ▶ The cloud service provider performs screening of potential employees before hiring e.g.: ○ References ○ CVs ○ Educational qualifications ○ Evaluation of employee trustworthiness	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for employing and observed, that the cloud service provider performs screening of potential employees before hiring. We have randomly inspected the latest employment and observed that proper screening has been made.	No deviations were found.
HR-02 - Employment and contractual conditions ▶ The cloud service provider's internal and external employees are obliged to comply with applicable guidelines and instructions relating to information security in their terms and conditions of employment and contract. ▶ The information security policy and the guidelines and instructions derived from it must be demonstrably acknowledged by the internal and external employees.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for employment and observed, that the employees are obliged to comply with guidelines and instructions. We have inspected by a random sample that employees have read and acknowledged relevant information security guidelines.	No deviations were found.
HR-03 - Safety training and awareness programme ▶ The cloud service provider holds awareness training of new employees in accordance with data protection and information security, in continuation of the employment. ▶ The cloud service provider conducts ongoing awareness training and quizzes of employees in accordance with information security and handling thereof.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider has a procedure for awareness training and observed that all new employees are required to participate. We have inspected by a random sample that new employees have been introduced to information security and have	No deviations were found.

Personnel (HR)

Objective

- *Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.*

Control activity	Test performed by BDO	Result of test
	read and acknowledged relevant information security guidelines. We have inspected by random samples that the cloud service provider conducts ongoing awareness training.	
HR-04 - Regulatory process ▶ Rules have been made for sanctions.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider has a procedure for sanctions	We have found that there have been no violations of policies or procedures. We have therefore not been able to test the implementation of this part of the control. No deviations were found.
HR-05 - Responsibilities in the event of termination or change of employment ▶ The cloud service provider has developed and implemented a procedure for offboarding retired employees. ▶ Upon resignation, the employee is informed that the signed confidentiality agreement is still valid.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider has a procedure for offboarding. For the most recently resigned employee, we have inspected that the cloud service provider has informed the resigned employee that the imposed duty of confidentiality still applies after termination of employment.	No deviations were found
HR-06 - Confidentiality agreements ▶ All employees have signed an employment contract containing a provision on professional secrecy ▶ External suppliers/consultants are subject to a duty of confidentiality when entering into a contract	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the cloud service providers procedure for employment and observed that it contains a segment on confidentiality for all employees.	No deviations were found

Personnel (HR)

Objective

- *Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.*

Control activity	Test performed by BDO	Result of test
	By a random sample, we have inspected that employees have signed a confidentiality clause in the employment contract. By inquiry we have been informed that the cloud service provider has no external employees with access to customer data.	

Asset Management (AM)

Objective

- *Identify the organisation’s own assets and ensure an appropriate level of protection throughout their lifecycle.*

Control activity	Test performed by BDO	Result of test
AM-01 - Inventory of the asset		
▶ The cloud service provider has set up procedures for inventorying the assets. ▶ The inventory is carried out by persons responsible for the assets in order to ensure complete, correct, valid and consistent recording over the life cycle of the assets. ▶ All data-carrying IT equipment must be purchased through the operational level to ensure that it is recorded. An inventory of all relevant devices connected to the cloud service providers IT infrastructure is maintained.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the that the cloud service provider has a procedure for inventorying the assets. We have inspected the procedure and observed that IT equipment must be purchased through the operational level. We have inspected that the inventory is maintained by relevant personnel to ensure complete, correct, valid and consistent recording over the life cycle of the assets.	No deviations were found
AM-02 - Guideline for the use and safe handling of assets		
▶ The cloud service provider has established guidelines and instructions for the authorised use and safe handling of assets.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the cloud service provider’s IT security handbook and observed that it contains guidelines and instructions for the use of assets. We have inspected by a random sample that new employees have read and acknowledged relevant information security guidelines. We have by random samples inspected that cloud service provider has implemented technical measures.	No deviations were found
AM-03 - Hardware commissioning		
▶ The cloud service provider has established guidelines and rules for the accepted use of assets and information.	We have conducted inquiries with appropriate personnel at the cloud service provider.	No deviations were found

Asset Management (AM)

Objective

- *Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.*

Control activity	Test performed by BDO	Result of test
▶ Operation and installment of servers is outsourced to the hosting provider according to the Operations and Maintenance Plan	We have inspected the cloud service provider's IT security handbook and observed that it contains guidelines and instructions for the use of assets. We have inspected by a random sample that new employees have read and acknowledged relevant information security guidelines. We have inspected the operations and maintenance plan and observed that it includes rules for servers. We have inspected that servers are hosted by Hetzner.	
AM-04 - Decommissioning of assets ▶ The cloud service provider has developed and implemented a procedure for disposing of media.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the cloud service providers procedure and observed it include a segment for disposing of media. By inquiry we have been informed that the cloud service provider has not disposed media.	We have found that the cloud service provider has not disposed of media. We have therefore not been able to test the implementation of this part of the control. No deviations were found.
AM-05 - Obligation for authorised use and safe handling of assets handed out and return ▶ Internal and external employees of the cloud service provider are demonstrably committed to the guidelines and instructions for the permitted use and secure handling of assets before they may be used. ▶ In connection with the termination of employment, handed over assets are returned.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the cloud service provider's IT security handbook and observed that it has established guidelines and instructions for the use of assets. We have inspected by a random sample that new employees have read and acknowledged relevant information security guidelines.	No deviations were found.

Asset Management (AM)

Objective

- *Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.*

Control activity	Test performed by BDO	Result of test
	We have inspected the cloud service providers procedure for employment and observed that assets are handed over after resignation. We have inspected by random sample that terminated employee's equipment is reset.	
AM-06 - Classification and labelling of assets - The cloud service provider has established procedures for classification of assets.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the overview of assets and observed all assets have the same classification.	No deviations were found.

Physical security (PS)

Objective

- *Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.*

Control activity	Test performed by BDO	Result of test
PS-01 - Security requirements for premises and buildings The cloud service provider ensures that the hosting provider has established physical perimeter security to protect areas that contain information. The physical perimeter security is in accordance with the adopted safety requirements.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the service provider's physical security policy. We have by physical inspection observed that the cloud service provider's entrance is locked ensuring only authorised people have access. We have inspected overview of who has access to the cloud service provider's office. We have inspected that servers are hosted by Hetzner. We have inspected that the cloud service provider oversees the hosting provider.	No deviations were found.
PS-02 - Redundancy model The cloud service provider ensures that the hosting provider has implemented procedures and controls to ensure redundancy in hosting environments.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that servers are hosted by Hetzner. We have inspected that the hosting provider has established physical security measures, including redundancy. We have inspected that the cloud service provider oversees the hosting provider.	No deviations were found.
PS-03 - Perimeter protection The cloud service provider ensures that the hosting provider has implemented procedures and controls for perimeter protection.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that servers are hosted by Hetzner.	No deviations were found.

Physical security (PS)

Objective

- *Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.*

Control activity	Test performed by BDO	Result of test
	We have inspected that the hosting provider has established physical security measures. We have inspected that the cloud service provider oversees the hosting provider.	
PS-04 - Access control - The cloud service provider ensures that the hosting provider has implemented procedures and controls to ensure sufficient access control management - The cloud service provider has established physical access controls, which prevent the likelihood of unauthorised access to the cloud service provider's offices, facilities and personal data, including ensuring that only authorised persons have access and all accesses are registered and logged.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that servers are hosted by Hetzner. We have inspected that the hosting provider has established physical security measures. We have inspected that the cloud service provider oversees the hosting provider. We have inspected the physical security policy. We have by physical inspection observed that the cloud service provider’s entrance is locked ensuring only authorised people have access. We have inspected overview of who has access to the cloud service provider’s office.	No deviations were found.
PS-05 - Protection against fire and smoke - The cloud service provider ensures that the hosting provider has implemented procedures and controls for protection against fire and smoke	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that servers are hosted by Hetzner. We have inspected that the hosting provider has established physical security measures, which include protection against fire and smoke.	No deviations were found.

Physical security (PS)

Objective

- *Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.*

Control activity	Test performed by BDO	Result of test
	We have inspected that the cloud service provider oversees the hosting provider.	
PS-06 - Protection against failure of the supply systems - The cloud service provider ensures that the hosting provider has implemented procedures and controls for protection against failure of the supply systems.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that servers are hosted by Hetzner. We have inspected that the hosting provider has established physical security measures, which include protection against failure of the supply systems. We have inspected that the cloud service provider oversees the hosting provider.	No deviations were found.
PS-07 - Monitoring of operating and environmental parameters - The cloud service provider ensures that the hosting provider has implemented procedures and controls for monitoring operating and environmental parameters.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that servers are hosted by Hetzner. We have inspected that the hosting provider has established physical security measures, which includes monitoring of operating and environmental parameters. We have inspected that the cloud service provider oversees the hosting provider.	No deviations were found.

Operation (OPS)

Objective

- *Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.*

Control activity	Test performed by BDO	Result of test
OPS-01 - Capacity management – Planning - The planning of capacities and resources follows an established procedure to avoid potential capacity bottlenecks. The procedures include forecasts of future capacity requirements in order to identify utilisation trends and manage risks of system overload.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected operation and maintenance plan and observed that it contains planning of capacity and resource management to avoid potential capacity bottlenecks. The procedure includes forecasts of future capacity requirements. We have inspected that the plan is approved by management. By physical inspection we have observed that the cloud service provider continuously monitors the capacity.	No deviations were found.
OPS-02 - Capacity management – monitoring - The cloud service provider has defined minimum up time for the cloud service provider, and this is monitored in real time.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected operation and maintenance plan and observed that it contains planning of capacity, uptime and performance. We have inspected that the procedure is approved by management. We have inspected that the cloud service provider's uptime is 99%. By physical inspection we have observed that the cloud service provider continuously monitors the capacity.	No deviations were found.
OPS-03 - Capacity management - control of resources - The cloud service provider receives reporting from the monitoring system and other tools which are used in the	We have conducted inquiries with appropriate personnel at the cloud service provider.	No deviations were found.

Operation (OPS)

Objective

- *Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.*

Control activity	Test performed by BDO	Result of test
planning of purchase of additional capacity. Data from monitoring is managed ad hoc.	We have inspected operation and maintenance plan and observed that it contains planning of capacity, uptime and performance. We have inspected that the procedure is approved by management. By physical inspection we have observed that the cloud service provider continuously monitors the capacity via screens in the office and sounds an alarm if any problems occur. We have by inquiry been informed that alarms are handled ad hoc.	
OPS-04 - Protection against malware – concept ▶ Controls are implemented for detection, prevention, and recovery to protect against malware, combined with appropriate user awareness.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the security description and security handbook and observed, that all units require updated malware protection. We have inspected by random sample that malware protection software is up to date. By inquiry we have been informed that the hosting provider is responsible for malware protection on servers. We have inspected by random samples that the cloud service provider conducts ongoing awareness training.	No deviations were found.
OPS-05 - Protection against malware – implementation ▶ Controls are implemented for detection, prevention, and recovery to protect against malware, combined with appropriate user awareness.	We have conducted inquiries with appropriate personnel at the cloud service provider.	No deviations were found.

Operation (OPS)

Objective

- *Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.*

Control activity	Test performed by BDO	Result of test
	We have inspected the security description and security handbook and observed, that all units require updated malware protection. We have inspected by random sample that malware protection software is up to date. By inquiry we have been informed that the hosting provider is responsible for malware protection on servers. We have inspected by random samples that the cloud service provider conducts ongoing awareness training.	
OPS-06 - Specifications for data backup and recovery – concept ▶ Systems and data are backed up daily and weekly. ▶ Daily backup is stored in 7 days and weekly in 12 weeks. ▶ Access to the backed-up data and the execution of restores is only carried out by authorised persons. ▶ Data is backed up in encrypted form in accordance with the latest state of the art.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the backup procedure and observed that backup of systems and data are required. We have inspected that the cloud service provider does daily and weekly backups and is carried out by authorised employees. We have inspected that backup data is encrypted.	No deviations were found.
OPS-07 - Data backup and restore – Monitoring ▶ Backup is stored separately from normal operation environments. ▶ The continuous backup is monitored. ▶ Faults are categorized and critical faults are rectified as fast as possible by qualified employees.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the backup procedure and observed that backup of systems and data are required. Furthermore, we have observed that the backup is monitored. We have inspected that backup data is stored separately.	We have found that there have been no alarms regarding the backups and restore. We have therefore not been able to test the implementation of this part of the control. No deviations were found.

Operation (OPS)		
Objective - *Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected that only qualified employees have access to backup and monitoring alarms.	
OPS-08 - Data backup and restore - Regular tests - Restore tests are performed once a year.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the contingency plans and observed that the cloud service provider performs restore test at least once a year. We have inspected that a retore test performed once a year.	No deviations were found.
OPS-09 - Data backup and restore – Storage - Systems and data transfers are encrypted via HTTPS and GPG keys.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that data at the hosting provider is encrypted. We have inspected that backup data is encrypted. We have inspected that Emento prod is encrypted by HTTPS.	No deviations were found.
OPS-10 - Logging and monitoring concept - All successful and unsuccessful attempts to access the cloud service provider's systems and data are logged. - All user changes in system and databases are logged.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud server provider has a procedure for logging. We have inspected by that all successful and unsuccessful attempts to access are logged.	No deviations were found.

Operation (OPS)

Objective

- *Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.*

Control activity	Test performed by BDO	Result of test
	We have inspected that all changes in system and databases are logged.	
OPS-11 - Logging and monitoring - concept for handling metadata ▶ The cloud service provider has established a clear concept for storing, handling and use of metadata in logs and monitoring systems related to the services.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud server provider's procedure for logging. We have inspected that the cloud service provider has established concept for storing, handling and use of metadata in logs and monitoring systems related to the services.	No deviations were found.
OPS-12 - Logging and monitoring - access, storage and deletion ▶ The cloud service provider has restricted who can access log data. ▶ Log data is stored in separate locations.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the cloud service providers procedure for logging and observed that access to log data is restricted. We have inspected that only employees with a work-related need have access to log data. We have observed that log data is stored in separate locations.	No deviations were found.
OPS-13 - Logging and monitoring - Detection of events ▶ Identified events are automatically reported to the personnel responsible or the responsible system compo-	We have conducted inquiries with appropriate personnel at the cloud service provider.	No deviations were found.

Operation (OPS)

Objective

▶ *Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.*

Control activity	Test performed by BDO	Result of test
nents of the cloud service provider in order to immediately assess the events and initiate the necessary measures.	By inquiry we have been informed that events are handled by the support team. We have inspected that the cloud service provider is notified automatically through alarms.	
OPS-14 - Logging and monitoring - Retention of logging data ▶ The cloud service provider stores logs in the “live log system” for 30 days - Live log system means the solution where logs are monitored. ▶ The cloud service provider stores raw log files for 6 months.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have observed that all successful and unsuccessful attempts to access are logged and stored for 30 days. We have inspected that all changes in system and databases are logged. We have observed that logs are stored for 6 months.	No deviations were found.
OPS-15 - Logging and monitoring – Attributability ▶ All successful and unsuccessful attempts to access the cloud service provider's systems and data are logged. ▶ All user changes in system and databases are logged.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have Inspected by live demonstration that all successful and unsuccessful attempts to access are logged. We have inspected that all changes in system and databases are logged.	No deviations were found.
OPS-16 - Logging and monitoring – Configuration ▶ The cloud service provider has restricted who can access log data.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for logging and observed that access to log data is restricted	No deviations were found.

Operation (OPS)		
Objective ▸ *Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected that the cloud service provider has granted access to log data only to authorised personnel.	
OPS-17 - Logging and monitoring - Availability of the monitoring software ▸ The cloud service provider reports information security weaknesses to relevant parties.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that information security weaknesses are reported to the customers in Emento Customernet.	No deviations were found.
OPS-18 - Dealing with weak points, faults and errors – concept ▸ The cloud service provider obtains information about technical vulnerabilities. ▸ The cloud service provider has taken a position on identified vulnerabilities.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the operation and maintenance plan and observed that the cloud service provider continuously conducts vulnerabilities tests. By inquiry we have been informed that vulnerabilities are taken care of ad hoc, if vulnerabilities can't be resolved instantly they are taken to TRUST meetings. We have inspected that the cloud service provider handles vulnerabilities through TRUST meetings.	No deviations were found.
OPS-19 - Dealing with vulnerabilities, faults and errors ▸ The cloud service provider obtains information about technical vulnerabilities. ▸ The cloud service provider has taken a position on identified vulnerabilities.	We have conducted inquiries with appropriate personnel at the cloud service provider.	No deviations were found.

Operation (OPS)		
Objective - *Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected the operation and maintenance plan and observed that the cloud service provider continuously conducts vulnerabilities tests. By inquiry we have been informed that vulnerabilities are taken care of ad hoc, if vulnerabilities can't be resolved instantly they are taken to TRUST meetings. We have inspected that the cloud service provider handles vulnerabilities through TRUST meetings.	
OPS-20 - Dealing with weak points, faults and errors - Measurements, analyses and evaluation of processes - The cloud service provider reports information security weaknesses to relevant parties.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that information security weaknesses are reported to the customers in Emento Customernet.	No deviations were found.
OPS-21 - Involvement of the cloud customer in the event of incidents - The cloud service provider reports information security incidents to relevant parties.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that information security weaknesses are reported to the customers in Emento Customernet.	No deviations were found.
OPS-22 - Testing and documentation of open vulnerabilities - The cloud service provider obtains information about technical vulnerabilities. - The cloud service provider has taken a position on identified vulnerabilities.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the operation and maintenance plan and observed that the cloud service provider continuously conducts vulnerabilities tests.	No deviations were found.

Operation (OPS)		
Objective - *Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.*		
Control activity	**Test performed by BDO**	**Result of test**
	By inquiry we have been informed that vulnerabilities are taken care of ad hoc, if vulnerabilities can't be resolved instantly they are taken to TRUST meetings. We have inspected that the cloud service provider handles vulnerabilities through TRUST meetings.	
OPS-23 - Dealing with weak points, faults and errors - System hardening - The cloud service provider has defined a procedure for hardening system components.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected operations and maintenance plan and observed that the cloud service provider has defined a procedure for hardening system components by various playbooks. We have observed that the procedure for hardening system components is implemented by various playbooks.	No deviations were found.
OPS-24 - Separation of data sets in the cloud infrastructure - Cloud customer data is stored securely and strictly separated in order to ensure the confidentiality and integrity of the data.	We have conducted inquiries with appropriate personnel at the cloud service provider. By inquiry we have been informed that servers at the hosting provider are separated. We have observed at site documentation that the cloud service provider actively has to change settings at the hosting provider which secures separation of data.	No deviations were found.

Identity and authorisation management (IDM)

Objective

- *Secure the authorisation and authentication of users of the Cloud Service Provider to prevent unauthorised access.*

Control activity	Test performed by BDO	Result of test
IDM-01 - Policy for access and access authorisations ▶ The cloud service provider has a roles and rights concept based on the cloud service provider's business and security requirements and a policy for managing access and access authorisations with the following specifications: ○ Assignment of unique usernames ○ Assignment and modification of access and access authorisations on the basis of the principle of least privilege and as required for the performance of tasks ○ Segregation of duties ○ Approval of the assignment or modification by authorised personnel ○ Regular review of assigned access and access authentications ○ Two- or multi-factor authentication for users with privileged access authentications.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the access control policy and IT security handbook and observed • that employees have unique usernames, • that access and authorisations are based on principle of least privilege, • that access rights are approved by authorised personnel, • that separation of duties is ensued, • that access rights are reviewed at least annually, • that multifactor authentication is required for users with privileged access. We have by a random sample inspected that the policy is implemented.	No deviations were found.
IDM-02 - Assigning and changing access and access authorisations ▶ The cloud service provider has set up a procedure for registering and deregistering the user in connection with the allocation of access rights.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the access control policy and IT security handbook and observed that access authorisations are assigned based on work related needs and are approved by authorised personnel. We have inspected by a random sample that access authorisations is approved by a superior. We have inspected by random sample that deregistering of access rights is done after resignation.	No deviations were found.

Identity and authorisation management (IDM)

Objective

- *Secure the authorisation and authentication of users of the Cloud Service Provider to prevent unauthorised access.*

Control activity	Test performed by BDO	Result of test
IDM-03 - Blocking and revocation of access authorisations in the event of inactivity or multiple failed logins - Technical Support users (2. level) are automatically created and assigned and may only be revoked by manual actions. - Customer Support users (1. level) are automatically created but must be manually assigned and revoked. - Both Technical Support and Customer Support users are controlled by manual configuration in the cloud service providers deployment process.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected Emento Flows and observed that the cloud service provider has established procedures for technical and customer support. We have inspected overview of technical support employees. We have inspected overview customer support employees. We have inspected that employees access rights are configured and controlled manually. We have inspected by a random sample that access authorisations is approved by a superior.	No deviations were found.
IDM-04 - Withdrawal or adjustment of access authorisations if the area of responsibility changes - Access authorisations are withdrawn promptly in the event of changes in the area of responsibility of the cloud service provider's internal and external employees.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the procedure for changes in authorisations and observed that authorisations are withdrawn immediately in the event of change in the area of responsibility. We have been informed by inquiry that no changes have been made since the implementation of the procedure.	We have found that no changes have been made since the introduction of the procedure. We have therefore not been able to test the implementation of the control. No deviations were found.
IDM-05 - Regular review of access authorisations - Users and user rights are checked at least once a year to ensure that they still correspond to the actual area of responsibility or use.	We have conducted inquiries with appropriate personnel at the cloud service provider.	No deviations were found.

Identity and authorisation management (IDM)

Objective

- *Secure the authorisation and authentication of users of the Cloud Service Provider to prevent unauthorised access.*

Control activity	Test performed by BDO	Result of test
	We have inspected that the cloud service provider has a procedure for reviewing user and user rights annually. We have inspected documentation that the cloud service provider has reviewed users and user rights according to the procedure.	
IDM-06 - Privileged access authorisations ▶ Privileged access authorisations for internal and external employees and technical users of the cloud service provider are assigned and changed in accordance with the policy for managing access and access authorisations. ▶ The activities of users with privileged access authorisations are logged in order to be able to detect any misuse of these authorisations in the event of suspicion.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the access control policy and IT security handbook and observed that access authorisations are assigned based on work related needs and are approved by authorised personnel. We have inspected vaults and observed there is a difference between ordinary authorisations and privileged authorisations. We have inspected by a random sample that privileged access authorisations is approved by a superior. We have observed that privileged access is logged.	No deviations were found.
IDM-07 - Access to cloud customer data ▶ The cloud service provider has support user access for selected employees (see IDM-03) which allows the cloud service provider to provide technical and customer support as needed. ▶ All support access is logged and can be inspected by the cloud customer on request.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the IT security description and observed that only authorised employees have access to customer data. We have inspected by random samples that privileged access authorisations is approved by management. We have inspected that support access is logged and that it can be inspected by customers.	No deviations were found.

Identity and authorisation management (IDM)

Objective

- *Secure the authorisation and authentication of users of the Cloud Service Provider to prevent unauthorised access.*

Control activity	Test performed by BDO	Result of test
IDM-08 - Confidentiality of authentication information ▶ The cloud service provider has developed procedures and controls for Confidentiality of authentication information.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider has developed a procedure for confidentiality of authentication. We have inspected the cloud service provider's password policy. We have inspected that all employees have two-factor authentication enabled.	No deviations were found.
IDM-09 - Authentication mechanisms ▶ The cloud service provider has established requirements for passwords which must be followed by all employees and external consultants. ▶ Access to the production environment requires two- or multi-factor authentication.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the Cloud service provider has developed a procedure for confidentiality of authentication. We have inspected the cloud service provider's password policy, which is enabled for all employees. We have inspected that all employees have two-factor authentication. We have inspected that multi-factor authentication is required when accessing production environment.	No deviations were found.

Cryptography and key management (CRY)

Objective

- *Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.*

Control activity	Test performed by BDO	Result of test
CRY-01 - Policy on the use of encryption methods and key management ▶ The cloud service provider has implemented an encryption policy for encryption of customer data. The policy defines the strength and protocol for encryption.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the cloud service provider's encryption policy and observed that it prescribes the strength and protocol for encryption. We have inspected that the procedure is implemented.	No deviations were found.
CRY-02 - Encryption of data during transmission (transport encryption) ▶ The cloud service provider has developed procedures and controls for encryption of data during transmission (transport encryption).	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the encryption policy and observed that the cloud service provider has a procedure for encryption during transmission. We have inspected that data is encrypted during transmission.	No deviations were found.
CRY-03 - Encryption of sensitive data during storage ▶ The cloud service provider has established procedures and technical measures for the encryption of cloud customers' data during storage.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the policy and observed that the cloud service provider has a procedure for encryption of data during storage. We have inspected documentation that the hosting providers storage of data is encrypted.	No deviations were found.

Cryptography and key management (CRY)

Objective

- *Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.*

Control activity	Test performed by BDO	Result of test
CRY-04 - Secure key management ▶ Processes and procedures are implemented for creation and maintenance of encryption keys to the customers.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the policy and observed that the cloud service provider has a procedure for key management. We have observed that keys are stored in 1password. By inquiry we have been informed that the CTO is managing keys and access to these.	No deviations were found.

Communication security (COS)		
Objective ▶ *Ensure the protection of information in networks and the corresponding information processing systems*		
Control activity	**Test performed by BDO**	**Result of test**
COS-01 - Technical protective measures ▶ The network topology is structured according to best-practice principles, which means that servers that run applications cannot be accessed directly from the Internet. ▶ The cloud service provider uses known network technologies and mechanisms (Firewall/Intrusion Detection-System) to protect internal networks.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the risk assessment and the security description and observed that the network is segmented which implies applications cannot be accessed directly from the internet. We have inspected that the cloud service provider uses IPS, logging and monitoring to protect internal network. We have observed that the cloud service provider has implemented alarms which are handled ad hoc.	No deviations were found.
COS-02 - Security requirements for connections in the cloud service provider's network ▶ The cloud service provider has implemented/required appropriate security measures to protect its network services.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the risk assessment and the security description and observed that the network is segmented which implies applications cannot be accessed directly from the internet. We have inspected that the cloud service provider uses IPS, logging and monitoring to protect internal network. We have observed that the cloud service provider has implemented alarms which are handled ad hoc.	No deviations were found.

Communication security (COS)

Objective

- *Ensure the protection of information in networks and the corresponding information processing systems*

Control activity	Test performed by BDO	Result of test
COS-03 - Monitoring of connections in the cloud service provider's network - The cloud service provider has developed procedures and controls for monitoring connections in the cloud service provider's network.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider uses known network technologies and mechanisms to protect internal network. We have observed that the cloud service provider has implemented alarms which are handled ad hoc.	No deviations were found.
COS-04 - Cross-network access - The cloud service provider has developed procedures and controls for cross-network access.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the security description and the customer service security responsibilities. We have observed how Emento Gateway allows customers to control what access they allow. We have inspected that multi-factor authentication is used when accessing with VPN connection.	No deviations were found.
COS-05 - Networks for administration - The cloud service provider has developed procedures and controls for networks for administration.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that access to servers and networks requires access through jump-global. We have inspected that admin access (SSH) is only allowed via jump host from Emento network (VPN).	No deviations were found.

Communication security (COS)

Objective

- *Ensure the protection of information in networks and the corresponding information processing systems*

Control activity	Test performed by BDO	Result of test
COS-06 - Segregation of data traffic in shared network environments The cloud service provider has developed procedures and controls for segregation of data traffic in shared network environments.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the security description and the customer service security responsibilities. We have observed how Emento Gateway allows customers to control what access they allow. We have inspected that multi-factor authentication is used when accessing with VPN connection.	No deviations were found.
COS-07 - Documentation of the network The cloud service provider has developed procedures and controls for documentation of the network.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the security description and observed that it prescribes the security architecture. We have inspected the risk assessment and the security description and observed that the network is segmented which implies applications cannot be accessed directly from the internet. We have inspected thar the network is segmented.	No deviations were found.
COS-08 - Data transmission policy The cloud service provider has developed procedures and controls for data transmission policy.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the encryption policy and observed that the cloud service provider has a procedure for encryption during transmission.	No deviations were found.

Communication security (COS)

Objective

- *Ensure the protection of information in networks and the corresponding information processing systems*

Control activity	Test performed by BDO	Result of test
	We have inspected that data is encrypted during transmission.	

Portability and interoperability (PI)

Objective

- *Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.*

Control activity	Test performed by BDO	Result of test
PI-01 - Documentation and safety of the input and output interfaces - The cloud service provider has implemented documentation in the form of system descriptions for all input and output interfaces.	We have conducted inquiries with appropriate personnel at the cloud service provider. By inquiry we have been informed that the cloud server provider has developed system description for all input and output interfaces. We have observed that all the descriptions are updated. By random samples we have inspected that input and output interfaces are described and updated.	No deviations were found.
PI-02 - Contractual agreements for the provision of data - The cloud service provider has implemented procedure for the contractual agreements on the provision of data upon termination of the agreement.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider has developed procedures for provision of data upon termination of the agreement. We have by inquiry been informed that there has been no termination of the agreement.	We have noted that there has been no termination of the agreement. We have therefore not been able to test the implementation of this part of the control. No deviations were found.

Portability and interoperability (PI)		
Objective ▶ *Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.*		
Control activity	**Test performed by BDO**	**Result of test**
PI-03 - Secure data erasure ▶ The cloud service provider has implemented procedures and controls for the secure data erasure.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider has developed procedures and controls for the secure data erasure. We have by inquiry been informed that there has been no termination of the agreement.	By inquiry we have been informed that there has been no termination of the agreement, we have therefore not been able to test the implementation of this part of the control. No deviations were found.

Procurement, development and modification of information systems (DEV)		
Objective - *Ensure information security in the development cycle of information systems.*		
Control activity	**Test performed by BDO**	**Result of test**
DEV-01 - Guidelines for the development / procurement of information systems - The cloud service provider has implemented procedures and controls for the development of systems and software in the organisation. - The guidelines and instructions contain specifications for the entire life cycle of the cloud service and are based on recognised standards and methods.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for change management. We have inspected the cloud service provider's checklist for secure development. We have inspected a random sample of a development task and observed that the procedure is followed and that the task starts with a risk assessment.	No deviations were found.
DEV-03 - Guidelines for the modification of information systems - The cloud service provider has implemented procedures for system changes.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for change management. We have inspected the cloud service provider's checklist for secure development. We have inspected a random sample of a development task and observed that the procedure is followed.	No deviations were found.
DEV-04 - Security training and awareness programme for continuous software deployment and associated systems, components or tools - The cloud service provider follows its established system change and system development procedures and regularly awareness-trains its employees on privacy-by-design and change management.	We have conducted inquiries with appropriate personnel at the cloud service provider. By inquiry we have been informed that all employees are required to sign the IT-security handbook.	No deviations were found.

Procurement, development and modification of information systems (DEV)		
Objective ▶ *Ensure information security in the development cycle of information systems.*		
Control activity	**Test performed by BDO**	**Result of test**
	By inquiry we have been informed that all developers follow the normal awareness training and top-up with targeted training. We have inspected by random sample that employees have signed that they read and the IT-security handbook. We have inspected that the cloud service provider has conducted awareness training for developers.	
DEV-05 - Risk assessment, categorisation and prioritisation of changes ▶ Changes are subjected to a risk assessment with regard to their potential impact on the affected system components and categorised and prioritised accordingly.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for change management. We have inspected the checklist for secure development. We have inspected a random sample of development tasks and observed that the procedure is followed, and that the task started with a risk assessment.	No deviations were found.
DEV-06 - Testing the changes ▶ Changes to the cloud service are subjected to suitable tests as part of software development and software provision.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for change management. We have inspected the checklist for secure development. We have inspected a random sample of development tasks and observed that the procedure is followed.	No deviations were found.

Procurement, development and modification of information systems (DEV)		
Objective *Ensure information security in the development cycle of information systems.*		
Control activity	**Test performed by BDO**	**Result of test**
DEV-07 - Logging of changes The cloud service provider has implemented automatic logging of changes in GitHub.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for change management. We have inspected relevant documentation and observed that changes in development tasks are logged.	No deviations were found.
DEV-08 - Version control The cloud service provider has implemented a setup for version history	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for change management. We have inspected that the cloud service provider has implemented a setup for version history.	No deviations were found.
DEV-09 - Approvals for deployment in the production environment The cloud service provider has established daily meetings for the development department where deployment of changes is agreed and approved.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have observed that the deployment is tested and approved before its deployed. By inquiry we have been informed that the development team discuss on daily meetings if the changes is going to the production environment. We have inspected that the cloud service provider has established daily meetings for the development.	No deviations were found.

Procurement, development and modification of information systems (DEV)

Objective

- *Ensure information security in the development cycle of information systems.*

Control activity	Test performed by BDO	Result of test
DEV-10 - Separation of the environments - Production environments are logically separated from test or development environments.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that production environments are logically separated from development environments.	No deviations were found.

Control and monitoring of service providers and suppliers (SSO)

Objective

- *Ensure the protection of information that service providers subcontractors can access and monitor the agreed services and security requirements.*

Control activity	Test performed by BDO	Result of test
SSO-01 - Guidelines and instructions for controlling and monitoring third parties - The cloud service provider has implemented guidelines and procedures for controlling and monitoring subcontractors. - The cloud service provider has established information security requirements for subcontractors used. - The cloud service provider has limited subcontractors' access to the cloud service provider's systems in relation to the subcontractor's work-related needs.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the supplier security policy and observed that the cloud service provider monitors subcontractors. Furthermore, we have observed that there is established requirements for the subcontractors' information security. We have inspected that the cloud service provider monitors their subcontractors. We have inspected the agreements with the subcontractors. We have inspected that agreements contain guidelines, which prescribes the same requirements for the subcontractors as the cloud service provider. By inquiry we have been informed that the subcontractors don't have access to the cloud server providers systems.	No deviations were found.
SSO-02 - Risk assessment of service providers and suppliers - Subcontractors of the cloud service provider are subject to a risk assessment in accordance with the guidelines and instructions for controlling and monitoring subcontractors before they contribute to the provision of the cloud service. - Risk assessment is reviewed regularly, at least once a year, by qualified personnel of the cloud service provider.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the supplier security policy and observed that the cloud service provider monitors subcontractors. Furthermore, we have observed that there is established requirements for the subcontractors' information security. We have inspected that the cloud service provider monitors subcontractors.	No deviations were found.

Control and monitoring of service providers and suppliers (SSO)

Objective

- *Ensure the protection of information that service providers subcontractors can access and monitor the agreed services and security requirements.*

Control activity	Test performed by BDO	Result of test
	We have inspected the risk assessment and observed that subcontractors are evaluated. We have inspected that the risk assessment is approved annually.	
SSO-03 - List of service providers and suppliers ▶ The cloud service provider registers subcontractors who contribute to the provision of cloud service. ▶ The list of subcontractors includes: ○ Company name ○ Company address ○ Locations of data processing and storage ○ Responsible contact person at the cloud service provider/supplier ○ Responsible contact person at the cloud service provider ○ Description of the service ○ Classification based on the risk assessment ○ Start of the benefit ○ Proof of compliance with the contractually agreed requirements. ▶ The information in the directory is checked at least once a year for completeness, accuracy and validity.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the supplier security policy and observed that the cloud service provider monitors subcontractors. Furthermore, we have observed that there is established a requirement for subcontractors' information security. We have inspected the list of subcontractors. We have inspected that it includes: ○ Company name ○ Company address ○ Locations of data processing and storage ○ Responsible contact person at the cloud service provider/supplier ○ Responsible contact person at the cloud service provider ○ Description of the service ○ Classification based on the risk assessment ○ Start of the benefit ○ Proof of compliance with the contractually agreed requirements. We have inspected that the cloud service provider monitors subcontractors annually.	No deviations were found.
SSO-04 - Monitoring compliance with the requirements ▶ The cloud service provider supervises subcontractors at least once a year, based on a risk assessment.	We have conducted inquiries with appropriate personnel at the cloud service provider.	No deviations were found.

Control and monitoring of service providers and suppliers (SSO)

Objective

- *Ensure the protection of information that service providers subcontractors can access and monitor the agreed services and security requirements.*

Control activity	Test performed by BDO	Result of test
	We have inspected the supplier security policy and observed that the cloud service provider monitors subcontractors. Furthermore, we have observed that there is established a requirement for subcontractors' information security. We have inspected that the cloud service provider monitors their subcontractors. We have inspected the risk assessment and observed that subcontractors are evaluated. We have inspected that the risk assessment is approved annually. We have inspected external audit reports from sub service providers.	
SSO-05 - Exit strategy for the receipt of benefits ▶ The cloud service provider has defined and documented exit strategies for the procurement of services for which the risk assessment of the cloud service providers and subcontractors revealed a very high dependency in terms of the scope, complexity and uniqueness of the procured service.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the cloud service provider's procedure for subcontractors and observed it includes strategies in the event of a subcontractors exit. We have by inquiry been informed that there have been no subcontractor exits.	We have found that there have been no exits, we have therefore not been able to test the implementation of this part of the control. No deviations were found.

Dealing with security incidents (SIM)

Objective

- *Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.*

Control activity	Test performed by BDO	Result of test
SIM-01 - Guideline for dealing with security incidents ▶ The cloud service provider has implemented a procedure for security breaches to ensure a fast, effective and proper response to all known security incidents. ▶ The cloud service provider has defined guidelines for the classification, prioritisation and escalation of security incidents.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for dealing with security incidents and observed that it includes a fast, effective and proper response to incidents. We have by inquiry been informed that no incidents have occurred since the introduction of the procedure.	We have found that no incidents have occurred since the introduction of the procedure, we have therefore not been able to test the implementation of this part of the control. No deviations were found.
SIM-02 - Processing of security incidents ▶ The procedure includes a process model and relevant concepts, guidelines and procedural instructions for dealing with security incidents.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for dealing with security incidents and observed that it includes handling and investigation of security incidents. We have by inquiry been informed that no incidents have occurred since the introduction of the procedure.	We have found that no incidents have occurred since the introduction of the procedure, we have therefore not been able to test the implementation of this part of the control. No deviations were found.
SIM-03 - Documentation and reporting of security incidents ▶ After processing a security incident, the solution is documented in accordance with the contractual agreements and the report is sent to the affected customers for final acknowledgement or, if necessary, as confirmation.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for dealing with security incidents and observed that it is required to report to the affected customers. We have by inquiry been informed that no incidents have occurred since the introduction of the procedure.	We have found that no incidents have occurred since the introduction of the procedure, we have therefore not been able to test the implementation of this part of the control. No deviations were found.

Dealing with security incidents (SIM)

Objective

- *Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.*

Control activity	Test performed by BDO	Result of test
SIM-04 - Obligation for users to report security incidents to a central office The cloud service provider shall inform employees and external business partners of their obligations.	We have conducted inquiries with appropriate personnel at the cloud service provider. By inquiry we have been informed that all employees are required to read and understand the IT-security handbook upon employment. We have inspected by a random sample that employees have read and understand issued policies and procedures regarding information security.	No deviations were found.
SIM-05 - Evaluation and learning process The cloud service provider learns from information security incidents and regularly reviews incidents and responses.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for dealing with security incidents and observed that it includes an evaluation process after incidents. We have by inquiry been informed that no incidents have occurred since the introduction of the procedure.	We have found that no incidents have occurred since the introduction of the procedure, we have therefore not been able to test the implementation of this part of the control. No deviations were found.

Business continuity and contingency management (BCM)

Objective

- *Plan, implement, maintain and test procedures and measures for business continuity and emergency management.*

Control activity	Test performed by BDO	Result of test
BCM-01 - Responsibility of the cloud service provider management ▶ The cloud service provider's top management is designated as the process owner of continuity and emergency management and is responsible for establishing the process within the organisation and ensuring compliance with the guidelines. They must ensure that sufficient resources are provided for an effective process.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider's top management is responsible for continuity and emergency management.	No deviations were found.
BCM-02 - Guidelines and procedures for business impact analysis ▶ The cloud service provider has established a contingency plan that ensures rapid response time to restore the availability of and access to personal information in a timely manner in the event of a physical or technical incident. ▶ The cloud service provider has established policies and procedures for determining the effects of disruptions to the cloud service.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the cloud service provider's contingency plan and observed that it ensures a rapid response time to avoid downtime and the compromise of information. We have inspected that the incident log describes the effects of disruptions to the cloud service.	No deviations were found.
BCM-03 - Business continuity planning ▶ The cloud service provider has implemented controls to ensure the continuity of information security. ▶ The cloud service provider has established BCM plans based on a business impact analysis and the Statement of Applicability. ▶ The contingency plan takes aspects from the criterion into account.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the cloud service provider's contingency plan and observed that it ensures a rapid response time to avoid downtime and the compromise of information. We have inspected that the contingency plan is based on a business impact analysis and the Statement of Applicability. We have inspected that the contingency plan and related action cards take aspects from the C5 criterion into account.	No deviations were found.

Business continuity and contingency management (BCM)		
Objective ▸ *Plan, implement, maintain and test procedures and measures for business continuity and emergency management.*		
Control activity	**Test performed by BDO**	**Result of test**
BCM-04 - Verification, updating and testing of business continuity ▸ The cloud service provider has established periodic testing of the contingency plan in order to ensure that the contingency plans are up-to-date and effective in critical situations. ▸ Contingency tests are documented and evaluated.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the cloud service provider's annual cycle and observed that a contingency plan test is conducted annually. We have inspected documentation that proves the test have taken place and evaluated. We have inspected the contingency plan is reviewed and approved annually.	No deviations were found.

Compliance (COM)

Objective

- *Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.*

Control activity	Test performed by BDO	Result of test
COM-01 - Identification of applicable legal, regulatory, self-imposed or contractual requirements - The cloud service provider has an overview of current legislation and contract requirements. - The cloud service provider regularly checks whether new rules affect the cloud service provider's treatment.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for identification of requirements and observed that the cloud service provider has an overview over current legislation and contract requirements. We have observed the approval of external requirements. We have inspected by a random sample that the cloud service provider regularly checks for new rules, threats or vulnerabilities through newsletters.	No deviations were found.
COM-02 - Guideline for planning and conducting audits - The cloud service provider has implemented procedures for planning and conducting audits.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider has procedures for planning and conducting internal and external audits. We have inspected compliance report conducted in June 2025.	No deviations were found.
COM-03 - Internal audits of the information security management system - The cloud service provider performs regular reviews of their policies. - The cloud service provider conducts internal audits annually.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that the cloud service provider reviews all their policies regularly.	No deviations were found.

Compliance (COM)

Objective

- *Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.*

Control activity	Test performed by BDO	Result of test
	We have inspected that the cloud service provider has procedures for planning and conducting internal and external audits. We have inspected compliance report conducted in June 2025.	
COM-04 - Information on the information security performance and management assessment of the ISMS ▶ The cloud service provider carries out regular reviews of the ISMS and relevant procedures and controls.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that ISMS is approved by top management. We have inspected documentation showing that the cloud service provider reviews all their policies regularly.	No deviations were found.

Dealing with investigative questions from government agencies (INQ)

Objective

- *Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.*

Control activity	Test performed by BDO	Result of test
INQ-01 - Legal assessment of investigation enquiries ▶ The cloud service provider has established guidelines and procedural instructions for dealing with and assisting with investigation requests from government agencies. ▶ Investigation enquiries are legally assessed by qualified personnel of the cloud service provider.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for handling inquiries from authorities and observed that the cloud service provider has established guidelines for dealing and assisting with investigation request from government agencies. We have by inquiry been informed that no request has been made since the introduction of the procedure.	We have found that no request has been made since the introduction of the procedure, we have therefore not been able to test the implementation of this part of the control. No deviations were found.
INQ-02 - Informing customers about investigation requests ▶ The cloud service provider immediately informs affected cloud customers, unless there are legal reasons to the contrary.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for handling inquiries from authorities and observed that cloud service provider has established guidelines for informing affected customers unless there are legal reasons to the contrary. We have by inquiry been informed that no request has been made since the introduction of the procedure.	We have found that no request has been made since the introduction of the procedure, we have therefore not been able to test the implementation of this part of the control. No deviations were found.
INQ-03 - Requirements for accessing or disclosing data in response to investigation requests ▶ The cloud service provider only provides access to or disclosure of cloud customers' data on the basis of a legal review.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for handling inquiries from authorities and observed that the cloud service provider only provides access to or disclosure of customers' data on the basis of a legal review. We have by inquiry been informed that no request has been made since the introduction of the procedure.	We have found that no request has been made since the introduction of the procedure, we have therefore not been able to test the implementation of this part of the control. No deviations were found.

Dealing with investigative questions from government agencies (INQ)

Objective

- *Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.*

Control activity	Test performed by BDO	Result of test
INQ-04 - Limitation of access to or disclosure of data in the event of investigation requests - In the event of the disclosure of customers' data, only the data that is the subject of the investigation request is disclosed. - If the data cannot be limited, the data is anonymised or pseudonymised.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the procedure for handling inquiries from authorities and observed that in case of disclosure, access to customer data is limited to only data that is the subject of investigation. We have inspected that data that cannot be limited is anonymised or pseudonymised. We have by inquiry been informed that no request has been made since the introduction of the procedure.	We have found that no request has been made since the introduction of the procedure, we have therefore not been able to test the implementation of this part of the control. No deviations were found.

Product safety (PSS)

Objective

- *Provides up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorisation of users of cloud customers.*

Control activity	Test performed by BDO	Result of test
PSS-01 - Guidelines and recommendations for cloud customers ▶ The cloud service provider has developed procedures for guidelines and recommendations for cloud customers' use of the service. ▶ The guidelines include instructions about secure configuration, updates, error handling and logging mechanisms, authentication mechanisms, roles and rights concepts, and administrative functions for the service.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the security description and observed, that the cloud service provider has developed a procedure for customer's use of service. By inquiry we have been informed that customers are given the cloud service providers security description. We have inspected the security description and observed that it includes instruction about secure configuration, updates, error handling and logging mechanisms, authentication mechanism, roles and rights concepts, and administrative functions.	No deviations were found.
PSS-02 - Identification of vulnerabilities of the cloud service ▶ The cloud service provider has developed procedures and controls for identification of vulnerabilities of cloud services. ▶ The procedures are part of the development process and include: static code analysis, dynamic code analysis, code reviews, and research of CVEs in authoritative libraries.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the security description and observed that the cloud service provider has implemented a procedure for vulnerabilities. We have inspected that cloud service provider proactively identifies vulnerabilities, through vulnerability test. We have inspected that vulnerabilities are evaluated.	No deviations were found.
PSS-03 - Online register of known vulnerabilities ▶ The cloud service provider offers a registry of known vulnerabilities (CVEs) for CVE's that the cloud service	We have conducted inquiries with appropriate personnel at the cloud service provider.	We have found that the cloud service provider offers a registry of incidents from the past 12 months, in which the level of

Product safety (PSS)

Objective

- *Provides up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorisation of users of cloud customers.*

Control activity	Test performed by BDO	Result of test
provider deems critical and are unable to resolve within an acceptable timeframe.	We have inspected the security description and observed that the cloud service provider has implemented a procedure for vulnerabilities. We have inspected that cloud service provider proactively identifies vulnerabilities, through vulnerability test. We have inspected that vulnerabilities are evaluated. We have inspected that the cloud service provider offers a registry of incidents for customers.	criticality is also specified. However, the list does not include Common Vulnerabilities and Exposures (CVEs). No further deviations were found.
PSS-04 - Feeder handling and logging mechanism ▶ The cloud service provider has implemented procedures and controls for error handling and logging mechanisms.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the cloud service provider's logging procedure and observed that it prescribes error handling and logging. We have inspected that the cloud service provider has implemented an alarm setup for error handling and logging.	No deviations were found.
PSS-05 - Authentication mechanisms ▶ The service offers mechanisms that can enforce strong authentication.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the security description and observed, that the customers can integrate the cloud service provider's mechanisms in their idP. We have by a random sample inspected the authentication mechanism between the cloud service provider's platform and a customer. We have observed that the customer is able to add multi-factor authentication.	No deviations were found.

Product safety (PSS)		
Objective ▶ *Provides up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorisation of users of cloud customers.*		
Control activity	**Test performed by BDO**	**Result of test**
PSS-06 - Session Management ▶ The services Default session timeouts are 8 hours for customer employees and 20 minutes for citizens/users. ▶ The cloud service provider offers integration to common AD solutions for customer managed session management.	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected that default session timeouts are 8 hours for customer employees. We have inspected that default session timeouts are 20 minutes for users. We have inspected that the cloud service provider offers integration to common AD solutions for customer managed session management.	No deviations were found.
PSS-07 - Confidentiality of authentication information ▶ The procedures include automatic changing of initial passwords, technical requirements for password strength (length and complexity). ▶ The cloud service provider offers integration into common AD solutions for customer managed authentication	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the security description and observed, that users can create their own passwords, if the solution is integrated with the customer's AD. We have by a random sample inspected, that the cloud service provider has implemented rules for passwords. We have observed that the customer is able to add multi-factor authentication.	No deviations were found.
PSS-08 - Roles and rights concept ▶ The cloud service provider provides a role and rights concept for customers. ▶ The cloud service provider offers integration into common AD solutions for customer managed roles and rights	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the security description and observed that the customer is offered a roles and rights concept.	No deviations were found.

Product safety (PSS)

Objective

- *Provides up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorisation of users of cloud customers.*

Control activity	Test performed by BDO	Result of test
	We have observed an overview over roles and rights and observed, that the customer manages their own roles and rights. We have observed that the cloud service provider is able to access as admin.	
PSS-09 - Authorisation mechanisms - The cloud service provider has implemented procedures and controls for authorisation mechanisms that ensure up-to-date access control. The functionality of all authorisation mechanisms is validated by the cloud service provider. - The cloud service provider offers integration into common AD solutions for customer managed authorisation	We have conducted inquiries with appropriate personnel at the cloud service provider. We have inspected the security description and observed, that users can create their own passwords, if the solution is integrated with the customer's AD. We have by a random sample observed, that the cloud service provider has implemented rules for passwords in the customers solution.	No deviations were found.
PSS-12 - Locations of data processing and storage - The cloud service provider discloses information of the location of the data processing to the customer.	We have conducted inquiries with appropriate personnel at the cloud service provider. By inquiry we have been informed that all data is stored at the hosting provider Hetzner in Nuremberg, Germany and Helsinki. We have by a random sample inspected a customer agreement and observed, that the hosting provider is listed.	No deviations were found.

BDO STATSAUTORISERET REVISIONSPARTNERSELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

BDO Statsautoriseret Revisionspartnerselskab, en danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO-netværk bestående af uafhængige medlemsfirmaer. BDO er varemærke for både BDO-netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.800 medarbejdere, mens det verdensomspændende BDO-netværk har ca. 95.000 medarbejdere i 169 lande.

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."

Allan Juhl
Direktør
Serienummer: f05ee19d-619d-4f3a-8665-0620bfc4b2e9
IP: 80.209.xxx.xxx
2026-02-06 08:51:28 UTC

Mit ID ✓

Nicolai Tobias Visti Pedersen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Statsautoriseret revisor
Serienummer: c42f66e9-59bb-478a-9d92-2a2b8602724e
IP: 77.243.xxx.xxx
2026-02-06 09:05:06 UTC

Mit ID ✓

Mikkel Jon Larssen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Partner
Serienummer: cd9a38dd-e75c-40f7-80d6-ec5b5d0841d6
IP: 93.82.xxx.xxx
2026-02-06 14:20:41 UTC

Mit ID ✓