SOFTWARE GMBH

Alfabet Cloud System

SOC 3 + HIPAA

System and Organization Controls (SOC) for Service Organizations Report
for the period of October 1, 2023 to September 30, 2024

Report of Independent Service Auditors issued by Aprio LLP

Table of Contents

I. Report of Independent Service Auditor

We have examined Software GmbH's (the "Company") accompanying assertion titled *Software GmbH's Assertion* (the "Assertion") indicating that the controls within the Alfabet Cloud System (the "System") were effective for the period of October 1, 2023 to September 30, 2024 (the "Specified Period"), to provide reasonable assurance that Software GmbH's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*), the applicable portions of the HIPAA Security Rule as defined in 45 CFR Part 160 and subparts A and C of Part 164 (the "HIPAA Criteria").

The Company uses Amazon Web Services (AWS), a subservice organization, Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses the Amazon Relational Database Service and AWS Simple Storage Service as a Platform-as-a-Service. Additionally, the Company uses Microsoft Azure, a subservice organization, as a Platform-as-a-Service for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company uses the Azure SQL Database and/or SQL Managed Instance service, as a Database-as-a-Service and uses the Office 365 as a Software-as-a-Service. Certain AICPA applicable trust Services criteria and the HIPAA Criteria specified in the section titled *Software GmbH's Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's Assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations. The Assertion does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's responsibilities

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *Software GmbH's Assertion* about the suitability of design and operating effectiveness of controls. When preparing its assertion, the Company is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and the HIPPA criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that the controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPPA criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the controls were not effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria and the HIPPA criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria and the HIPPA criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPPA criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other matters

We did not perform any procedures regarding the fairness of presentation as it relates to the description criteria of the description in Section III titled *Software GmbH's Description of the Boundaries of its System*, and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, Software GmbH's assertion that the controls within the Company's System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPPA criteria, in all material respects, is fairly stated.

Aprio, LLP

Aprio, LLP

Atlanta, Georgia
December 3, 2024

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations
™

II. Software GmbH’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over Software GmbH’s (the “Company”) Alfabet Cloud System (the “System” or “Alfabet”) for the period of October 1, 2023 to September 30, 2024 (the “Specified Period”), to provide reasonable assurance that the Company’s service commitments and system requirements relevant to Security and Availability were achieved. We have performed an evaluation of the effectiveness of the controls within the System throughout the Specified Period to provide reasonable assurance that the Company’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (the “applicable trust services criteria”) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*) and the applicable portions of the HIPAA Security Rule as defined in 45 CFR Part 160 and subparts A and C of Part 164 (the “HIPAA Criteria”). The Company’s objectives for the system in applying the applicable trust services criteria and the HIPAA Criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria and the HIPAA criteria. The principal service commitments and system requirements related to the applicable trust services criteria and the HIPAA Criteria are specified in the section titled *Software GmbH’s Description of the Boundaries of its System*.

The Company uses Amazon Web Services (AWS), a subservice organization, Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses the Amazon Relational Database Service and AWS Simple Storage Service as a Platform-as-a-Service. Additionally, the Company uses Microsoft Azure, a subservice organization, as a Platform-as-a-Service for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company uses the Azure SQL Database and/or SQL Managed Instance service, as a Database-as-a-Service and uses the Office 365 as a Software-as-a-Service. Certain AICPA applicable trust services criteria and the HIPAA Criteria specified in the section titled *Software GmbH’s Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company’s controls are suitably designed and operating effectively, along with related controls at the Company. Management’s assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the System were effective throughout the Specified Period to provide reasonable assurance that the Company’s service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPPA criteria.

III. Software GmbH's Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of Software GmbH (the "Company") as it relates to its Alfabet Cloud System (the "System") for the period of October 1, 2023 to September 30, 2024 (the "Specified Period") for the trust services criteria relevant to Security and Availability ("applicable trust services criteria") as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*), the applicable portions of the HIPAA Security Rule as defined in 45 CFR Part 160 and subparts A and C of Part 164 (the "HIPAA Criteria").

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

B. Company Overview and Background

Software GmbH is a software company which enables enterprises to connect any technology - clouds, apps, devices, and data - anywhere and any way they choose.

Software GmbH was founded in 1969. The Company's headquarters is located in Darmstadt, Germany. Software GmbH offers a comprehensive suite of software products encompassing Internet of Things and self-service analytics, integration, APIs and business transformation. For more information visit softwareag.com.

C. System Overview

1. Infrastructure

Key IaaS provider infrastructure service components and monitoring services supporting the delivery of Cloud Services are described in the Subservice Organizations section.

The applicable sub-service organizations are included in this document as service descriptions of respective IaaS providers.

Supporting Systems Overview

Alfabet helps organizations make better IT investment decisions and reduces transformational risks by understanding the suitable parameters to make changes to their IT portfolio. It links the interdependent perspectives of IT, business, finance, and risk for "whole view" analysis of how IT can support business change. Enterprise architecture capabilities build the necessary foundation with an accurate, real-time picture of the IT landscape, including all applications and technologies, the inter-relationships between them, the information they exchange as well as the business capabilities and processes they support. Alfabet's portfolio management capabilities support independent decision-making for optimization of individual portfolios as well as portfolio- level strategy modelling to incorporate all portfolios into strategy formulation. Its collaborative planning platform helps enable all stakeholders to interface, communicate and consider multiple perspectives when making transformation decisions as well as prioritize project proposals based on alignment with business strategy. Alfabet is available as an on-premise or SaaS solution.

Systems Overview	Purpose
Amazon Web Services	System Infrastructure
Linux	Operating System
Microsoft Windows	Operating System
AWS Relational Database Service (RDS)	Cloud Database Service
AWS Simple Storage Service (S3)	Cloud Object Storage
Microsoft Azure	System Infrastructure
Azure SQL Database	Cloud Database Service
Microsoft SQL Server	Data warehousing
Active Directory	Identity Management

2. Software and Supporting Software Tools

Security and Monitoring Software

Key components supporting the delivery of cloud services include:

- *IaaS Provider:* The IaaS Provider(s) provides security and monitoring services as outlined in Parts 9 and 10 of this section of the report.
- *CrowdStrike Falcon:* CrowdStrike Falcon provides cloud workload and endpoint security, threat intelligence, and cyberattack response services.

  See https://www.CrowdStrike.com/
- *Okta:* Okta is one trusted platform to secure every identity, from customers to the Company's workforce, with Single Sign-On, Multi-factor Authentication, Lifecycle Management, and more.

  See https://www.okta.com/
- *Rapid7 InsightCloudSec:* InsightCloudSec is Cloud Security Posture Management (CSPM) tool which assesses cloud environments for security misconfigurations and policy compliance violations.

  See https://www.rapid7.com/products/insightcloudsec/
- *Microsoft Sentinel:* Microsoft Sentinel is a SIEM solution which provides real-time analysis of security alerts.

  See https://azure.microsoft.com/en-us/services/microsoft-sentinel/#overview
- *KeePassXC:* KeePassXC is a free open-source password manager which helps in managing passwords in a secure way. All passwords are kept in one database which is locked with one master key or a key file. The database is encrypted.
- *Duo Security*: Duo Security's Access platform is verifying the identity of users and the health of devices before they connect to applications.
- *Akamai*: Akamai provides Enterprise Application Access (EAA) management.

In addition, the Alfabet Cloud System leverages the following supporting software tools:

- *JumpCloud:* JumpCloud is an identity and access management solution used for portions of the in-scope system.
- *Qualys:* Qualys is a vulnerability scanning solution.

- *Microsoft Defender:* Defender is a threat detection and response solution.
- *Grafana:* Grafana is an analytics and monitoring solution.
- *Prometheus:* Prometheus is an event monitoring and alerting solution.
- *OpsGenie:* OpsGenie is an alerting and incident response tool.
- *GitHub:* GitHub is a source code control solution.

Management Software

The following services components are provided to facilitate the delivery of Cloud services.

- *Confluence (iWiki):* Confluence is a team collaboration software which is used by Cloud Operations to create and manage operational documentation (iWiki).

  See https://www.atlassian.com/software/confluence

- *Jira (iTrac):* iTrac is the Cloud Operations (CloudOps) and RnD bug fix and change management ticketing system. Customer incidents can be escalated to iTrac from Jira Service Management by the Global Support team or directly entered as incidents are identified.

  See https://www.atlassian.com/software/jira

- *Jira Service Management/Empower*: Jira Service Management/Empower is the support incident tool of Software GmbH. All incidents of Cloud customers are logged via Empower and worked on in Jira Service Management. Cloud Support Manager or Cloud Support Expert checks support incidents for cloud-specific properties and forwards them to Cloud Service Operations as required. The status of the incident is communicated via Empower to the customer.

3. People

Software GmbH Cloud *Information security roles and responsibilities*

- *Chief Information Security Officer Office* (CISO Office) is a centralized unit which is responsible to initiate and control the implementation and operation of information security within the Software GmbH Organization.
- *Cloud Operations (CloudOps) is an informal unit, part of the respective product BU, coordinating the* activities related to service operations for Standard Cloud Services and includes the following vital roles which are described in further detail in the Cloud ISMS A6 Organization of Information security.
- *Head of Business Unit (BU) Cloud Services is* responsible for team management, coordination of service delivery, and compliance with cloud policies. This role conducts procedure reviews and participates in regular advisory sessions for change management and risk assessment.
- *Cloud Operations System Owners*
  - Cloud Delivery: Provides cloud product specific team leadership and is responsible for day-to-day management and coordination of running the service. This role is the ultimate point of escalation for product specific cloud operations issues.
  - Infrastructure: Manages Cloud IaaS Infrastructure operational relationships for respective providers and provides common services applicable to all cloud systems.
  - Automation: Delivers Infrastructure-as-code and provides cloud service specific baseline.
- *Cloud Operations Engineer/Cloud DevOps Engineer:*

  The Cloud Operations Engineer is a supporting role for various cloud operations tasks and the duties include but are not limited to:

  - Cloud Service Management
  - Cloud Service Administration

Members of CloudOps are located globally in Software GmbH offices in Germany, Bulgaria, USA, Australia, Malaysia, and India. CloudOps is distributed in different time zones to provide "follow the sun" coverage for customer's support needs and to offer maintenance windows outside of customer's standard business hours.

Management and Board of Directors

The Supervisory Board collaborates with the Software GmbH Management Board to fulfill its advisory role as required by law and by the Company's articles of incorporation. The Supervisory Board advises the Management Board in aspects of running the Company and supervises work performed by the Management Board. In doing so, the Supervisory Board is directly involved in all decisions of key relevance to Software GmbH. The Management Board informs the Supervisory Board regularly, comprehensively, and promptly regarding all important aspects of strategy, the status of strategy implementation, planning, business development, the risk situation and risk management, and compliance via oral and written reports. The Management Board is also available to the Supervisory Board in meetings for questions and discussions where any deviations from planned business development is explained in detail.

External Suppliers

IaaS providers' services are described in Parts 9 and 10 of this section of the report. For each new supplier, the Security team determines the vendors risk-rating based on the supplier level of access, the sensitivity of the related data, and the impact to the operations in accordance with the Provisioning and Management Standard for IT Applications and Supplier Services. Suppliers with access to confidential data are subject to a detailed review that covers security controls such as SOC 2 attestations and/or applicable Information Security Certifications. On an annual basis, suppliers who have access to confidential data and/or who perform a managed service related to the operation of the systems are subjected to continuous monitoring controls as described above. Corrective actions are taken, if necessary. The Provisioning and Management Standard for IT Applications and Supplier Services policy governs the performance of suppliers that support the delivery of the Software GmbH Cloud Services. Members of the Information Security and Data Functions are responsible for reviewing and approving suppliers to help ensure that they comply with the relevant security and availability practices and commitments.

Internal Suppliers

CloudOps interacts with several other Software GmbH teams to provide the Standard Cloud services.

- *Research and Development (RnD):* RnD develops and releases new product versions four times per year. They participate in regular Cloud change advisory board meetings to review change management and security topics. Product related customer incidents may be escalated to RnD through an iTrac ticket.
- *Global Support:* Global Support is the single point of contact for Cloud Customers. All support requests are initially managed by a Global Support Customer Support Representative (CSR). If support cannot solve an incident directly, the incident is escalated to either CloudOps for cloud platform related issues or to R&D for product related issues.
- *Product Management:* Product Management prioritizes new features for Software GmbH. They interface between RnD, CloudOps, Marketing, and Sales for Cloud topics.
- *Information Technology (IT):* The team provides IT services to CloudOps such as Communication, Security Operations Center, Physical Asset Management, and Networking for day-to-day business activities. They also administer basic access and use of Software AG Information systems.
- *Contract Management and Legal:* The CM&L Team is responsible for handover of a new contract to the CloudOps Team as a basis for delivering the service.

4. Data

Data Privacy and Protection

Aligned with General Data Protection Regulation (GDPR) requirements and as documented in the Privacy Policy for Standard & Managed Cloud Services, the Software GmbH Data Privacy Office (dataprotection@softwareag.com) is the contact for customers and authorities regarding data privacy.

Customer Account Information

The customer is required to create an account to access and use the Services. To create an Account, the customer must provide certain personal information about the user and create a username and password. The customer is responsible for maintaining the confidentiality of its username and password and agrees to notify CloudOps if its password is lost, stolen, or disclosed to an unauthorized third party or otherwise may have become compromised. The customer is responsible for all activities that occur under its Account.

Access to Tenant Data

Application user accounts are created during onboarding and are under the responsibility of the customer. Customers are responsible for end-user administrative privileges within the Cloud Service tenant and have control over who is authorized to access the customer's environment. CloudOps personnel access to tenant data requires customer consent.

In case of a support incident requiring access to the customer’s Cloud Product tenant data, the customer can choose to grant access to CloudOps to examine the issue by providing user credentials, function privileges, and client licenses to access the data. All customer tenant content is directly encapsulated in the logically segregated tenant database.

IaaS Infrastructure

Customer tenant data is stored only inside the IaaS provider environment within the Cloud Product Service (at runtime) and the database and file storage (rest). Processing of tenant content is directly encapsulated in the cloud application accessed via the cloud service.

Only the CloudOps and other authorized Software GmbH support groups have access to the IaaS hosted environments with the least privileges and two-factor authentication. All-access attempts and activities within the hosted environments are logged using CloudOps monitoring and IaaS provider services. Physical security is the responsibility of the IaaS provider as outlined in the Subservice Organizations section of the report.

D. Principal Service Commitments and System Requirements

Software GmbH designs its processes and procedures related to its Alfabet Cloud System services to achieve the Company’s objectives. Those objectives are based on the service commitments that Software GmbH makes to user entities, the laws and regulations that govern the provision of the Alfabet Cloud System, and the operational, and HIPAA compliance requirements that Software GmbH has established for the services. Security and availability commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offerings provided online. Security and availability commitments are standardized and include, but are not limited to, the following:

- The use of the security principle that is designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role;
- The use of encryption technologies to protect customer data in transit over untrusted networks;
- The use of reasonable precautions to protect the security of the information that is collected; and
- The use of the availability principle that is designed to help ensure the availability of the systems supporting the Alfabet Cloud System.

Software GmbH establishes operational requirements that support the achievement of security and availability commitments, relevant laws and regulations, HIPAA compliance requirements, and other system requirements. Such requirements are communicated in Software GmbH's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected.

E. Non-Applicable Trust Services Criteria

Security and Availability Trust Services Categories		
Non-Applicable Trust Services Criteria		Software GmbH's Rationale
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	N/A – The Company's hosting providers, Amazon Web Services (AWS) and Microsoft Azure (Azure), are responsible for physical security controls. The Company does not maintain any hard copy data or store any customer information physically.

F. Subservice Organizations

The Company utilizes a subservice organization to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party subservice organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organizations and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organizations. Each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Amazon Web Services (AWS)	The Company uses Amazon AWS Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses the Amazon Relational Database Service (Amazon RDS) and AWS Simple Storage Service (S3) as a Platform-as-a-Service. Amazon RDS is more specifically a Database-as-a-Service. Amazon S3 provides object storage through a web service interface. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression;	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over managing infrastructure security such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the physical servers supporting the Infrastructure-as-a-Service Platform; • Controls over the configuration settings within the EC2 instance to ensure that data is encrypted and stored as per the configuration settings selected with AWS; • Controls over incident monitoring, response, and follow up; • Controls over managing the Platform-as-a-Service components (Amazon RDS and S3) such as physical servers and operating systems including applying critical patching for this infrastructure; • Controls over Amazon RDS and S3 including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; • Controls around AWS S3 redundancy, including controls over data replication; and • Controls around the change management processes for the AWS Infrastructure-as-a-Service Platform and the Platform-as-a-Service Platform (RDS and S3) components as applicable. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On an annual basis, the Information Security Function evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary, and • On a daily basis, CloudOps performs full file-based backups for each product to verify the integrity of the backup data.	CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3*
Microsoft Azure	The Company uses Microsoft Azure’s Platform-as-a-Service for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses the Azure SQL Database and/or SQL Managed Instance service, which is a Platform-as-a-Service or more specifically a Database-as-a-Service. The Company also uses Microsoft’s Office 365’s Software-as-a-Service. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing the security of infrastructure and Software including Azure SQL Database and/or SQL Managed Instance service such as physical servers and physical access to backups and facilities;	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over the change management processes for the Software and infrastructure supporting the platform including Azure SQL Database and/or SQL Managed Instance service; • Controls over incident monitoring, response, and follow up; • Controls over the prevention, detection, and follow up upon the introduction of malicious Software; • Controls over Azure Storage redundancy, including controls over data replication; • Controls over the encryption of transmitted and stored data within the platform including Azure SQL Database and/or SQL Managed Instance service; and • Controls over managing patching for the Software and infrastructure supporting the platform, including Azure SQL Database and/or SQL Managed Instance service. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On an annual basis, the Information Security Function evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary, and • On a daily basis, CloudOps performs full file-based backups for each product to verify the integrity of the backup data.	CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3*

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at this subservice organization that support the service organization's service commitments and system requirements are in place and are operating effectively.*

G. Cross-referencing of the SOC 2 Criteria to the HIPAA Criteria

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Administrative Safeguards	§164.308 Administrative safeguards.	
Administrative Safeguards	§164.308(a) A covered entity or business associate must, in accordance with §164.306:	
Administrative Safeguards	§164.308(a)(1)(i) **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.	CC 1.1
Administrative Safeguards	§164.308(a)(1)(ii) **Implementation specifications:**	

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Administrative Safeguards	§164.308(a)(1)(ii)(A) **Risk analysis (Required).** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	CC 2.1
Administrative Safeguards	§164.308(a)(1)(ii)(B) **Risk management (Required).** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	CC 2.1 CC 2.1
Administrative Safeguards	§164.308(a)(1)(ii)(C) **Sanction policy (Required).** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	CC 1.1
Administrative Safeguards	§164.308(a)(1)(ii)(D) **Information system activity review (Required).** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	CC 2.1 CC 4.2 CC 4.2
Administrative Safeguards	§164.308(a)(2) **Standard: Assigned security responsibility.** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	CC 1.3
Administrative Safeguards	§164.308(a)(3)(i) **Standard: Workforce security.** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	CC 1.1
Administrative Safeguards	§164.308(a)(3)(ii) **Implementation specifications:**	
Administrative Safeguards	§164.308(a)(3)(ii)(A) **Authorization and/or supervision (Addressable).** Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	CC 6.2
Administrative Safeguards	§164.308(a)(3)(ii)(B) **Workforce clearance procedure (Addressable).** Implement procedures to determine that the access of a workforce member to electronic protected health information **is appropriate.**	CC 6.2
Administrative Safeguards	§164.308(a)(3)(ii)(C) **Termination procedures (Addressable).** Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	CC 6.1

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Administrative Safeguards	§164.308(a)(4)(i) **Standard: Information access management.** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	CC 1.1
Administrative Safeguards	§164.308(a)(4)(ii) **Implementation specifications:**	
Administrative Safeguards	§164.308(a)(4)(ii)(A) **Isolating health care clearinghouse functions (Required).** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	N/A, Software GmbH is not a healthcare clearinghouse.
Administrative Safeguards	§164.308(a)(4)(ii)(B) **Access authorization (Addressable).** Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	CC 6.2
Administrative Safeguards	§164.308(a)(4)(ii)(C) **Access establishment and modification (Addressable).** Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	CC 6.2 CC 6.2
Administrative Safeguards	§164.308(a)(5)(i) **Standard: Security awareness and training.** Implement a security awareness and training program for all members of its workforce (including management).	CC 1.4
Administrative Safeguards	§164.308(a)(5)(ii) **Implementation specifications. Implement:**	
Administrative Safeguards	§164.308(a)(5)(ii)(A) **Security reminders (Addressable).** Periodic security updates.	CC 5.2
Administrative Safeguards	§164.308(a)(5)(ii)(B) **Protection from malicious software (Addressable).** Procedures for guarding against, detecting, and reporting malicious software.	CC 2.1 CC 6.8 CC 6.8
Administrative Safeguards	§164.308(a)(5)(ii)(C) **Log-in monitoring (Addressable).** Procedures for monitoring log-in attempts and reporting discrepancies.	CC 2.1 CC 6.6
Administrative Safeguards	§164.308(a)(5)(ii)(D) **Password management (Addressable).** Procedures for creating, changing, and safeguarding passwords.	CC 6.1
Administrative Safeguards	§164.308(a)(6) (i) **Standard: Security incident procedures.** Implement policies and procedures to address security incidents.	CC 1.1 CC 4.2 CC 4.2

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Administrative Safeguards	§164.308(a)(6)(ii) **Implementation specification: Response and reporting (Required).** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	CC 1.1 CC 4.2
Administrative Safeguards	§164.308(a)(7)(i) **Standard: Contingency plan.** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	CC 7.5
Administrative Safeguards	§164.308(a)(7)(ii) **Implementation specifications:**	
Administrative Safeguards	§164.308(a)(7)(ii)(A) **Data backup plan (Required).** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	CC 7.5
Administrative Safeguards	§164.308(a)(7)(ii)(B) **Disaster recovery plan (Required).** Establish (and implement as needed) procedures to restore any loss of data.	CC 7.4 CC 7.5
Administrative Safeguards	§164.308(a)(7)(ii)(C) **Emergency mode operation plan (Required).** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	CC 7.5
Administrative Safeguards	§164.308(a)(7)(ii)(D) **Testing and revision procedures (Addressable).** Implement procedures for periodic testing and revision of contingency plans.	CC 7.5
Administrative Safeguards	§164.308(a)(7)(ii)(E) **Applications and data criticality analysis (Addressable).** Assess the relative criticality of specific applications and data in support of other contingency plan components.	CC 7.5
Administrative Safeguards	§164.308(a)(8) **Standard: Evaluation.** Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	CC 1.1 CC 1.3

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Administrative Safeguards	§164.308(b)(1) **Business associate contracts and other arrangements.** A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	CC 1.3
Administrative Safeguards	§164.308(b)(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	CC 1.3
Administrative Safeguards	§164.308(b)(3) **Implementation specifications: Written contract or other arrangement (Required).** Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).	CC 1.3
Physical Safeguards	§164.310 Physical safeguards.	
Physical Safeguards	§164.310 A covered entity or business associate must, in accordance with §164.306	
Physical Safeguards	§164.310(a)(1) **Standard: Facility access controls.** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	N/A - Physical security is the responsibility of the IaaS provider.
Physical Safeguards	§164.310(a)(2) **Implementation specifications:**	
Physical Safeguards	§164.310(a)(2)(i) **Contingency operations (Addressable).** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	CC 7.5 CC 7.5
Physical Safeguards	§164.310(a)(2)(ii) **Facility security plan (Addressable).** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	N/A - Physical security is the responsibility of the IaaS provider.
Physical Safeguards	§164.310(a)(2)(iii) **Access control and validation procedures (Addressable).** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	N/A - Physical security is the responsibility of the IaaS provider.

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Physical Safeguards	§164.310(a)(2)(iv) **Maintenance records (Addressable).** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	N/A - Physical security is the responsibility of the IaaS provider.
Physical Safeguards	§164.310(b) **Standard: Workstation use.** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	CC 1.1
Physical Safeguards	§164.310(c) **Standard: Workstation security.** Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	N/A - Workstation security is addressed through authentication controls to the IaaS Platforms.
Physical Safeguards	§164.310(d)(1) **Standard: Device and media controls.** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	N/A - Management of hardware and electronic media is the responsibility of the IaaS service providers.
Physical Safeguards	§164.310(d)(2) **Implementation specifications:**	
Physical Safeguards	§164.310(d)(2)(i) **Disposal (Required).** Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	CC 6.5
Physical Safeguards	§164.310(d)(2)(ii) **Media re-use (Required).** Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	N/A - Management of hardware and electronic media is the responsibility of the IaaS service providers.
Physical Safeguards	§164.310(d)(2)(iii) **Accountability (Addressable).** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	N/A - Management of hardware and electronic media is the responsibility of the IaaS service providers.
Physical Safeguards	§164.310(d)(2)(iv) **Data backup and storage (Addressable).** Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	N/A - Management of hardware and electronic media is the responsibility of the IaaS service providers.
Technical Safeguards	§164.312 Technical safeguards.	
Technical Safeguards	§164.312 A covered entity or business associate must, in accordance with §164.306:	

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Technical Safeguards	§164.312(a)(1) **Standard: Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	CC 1.1 CC 6.1 CC 6.2 CC 6.2
Technical Safeguards	§164.312(a)(2) **Implementation specifications:**	
Technical Safeguards	§164.312(a)(2)(i) **Unique user identification (Required).** Assign a unique name and/or number for identifying and tracking user identity.	CC 5.2
Technical Safeguards	§164.312(a)(2)(ii) **Emergency access procedure (Required).** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	CC 7.5 CC 7.5
Technical Safeguards	§164.312(a)(2)(iii) **Automatic logoff (Addressable).** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	CC 6.1
Technical Safeguards	§164.312(a)(2)(iv) **Encryption and decryption (Addressable).** Implement a mechanism to encrypt and decrypt electronic protected health information.	CC 6.1 CC 6.7
Technical Safeguards	§164.312(b) **Standard: Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	CC 2.1
Technical Safeguards	§164.312(c)(1) **Standard: Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	CC 1.1 CC 6.1 CC 6.2 CC 6.2 CC 6.5
Technical Safeguards	§164.312(c)(2) **Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).** Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	CC 2.1 CC 6.1
Technical Safeguards	§164.312(d) **Standard: Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	N/A - Software GmbH does not interact with data subjects and is not responsible for providing access to electronic protected health information to data subjects.
Technical Safeguards	§164.312(e)(1) **Standard: Transmission security.** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	CC 6.1 CC 6.6 CC 6.7

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Technical Safeguards	§164.312(e)(2) **Implementation specifications:**	
Technical Safeguards	§164.312(e)(2)(i) **Integrity controls (Addressable).** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	CC 6.1 CC 6.6 CC 6.7
Technical Safeguards	§164.312(e)(2)(ii) **Encryption (Addressable).** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	CC 6.1 CC 6.7
Organizational Safeguards	§164.314 Organizational requirements.	
Organizational Safeguards	§164.314(a)(1) **Standard: Business associate contracts or other arrangements.** The contract or other arrangement required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.	CC 1.3
Organizational Safeguards	§164.314(a)(2) **Implementation specifications (Required).**	
Organizational Safeguards	§164.314(a)(2)(i) **Business associate contracts.** The contract must provide that the business associate will adhere to the requirements of the subparts below.	
Organizational Safeguards	§164.314(a)(2)(i)(A/B) In accordance with §164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and	CC 1.3 CC 1.3
Organizational Safeguards	§164.314(a)(2)(i)(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.	CC 1.3 CC 1.3
Organizational Safeguards	§164.314(a)(2)(ii) **Other arrangements.** The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of §164.504(e)(3).	CC 1.3
Organizational Safeguards	§164.314(a)(2)(iii) **Business associate contracts with subcontractors.** The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	CC 1.3

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Organizational Safeguards	§164.314(b) (1) **Standard: Requirements for group health plans.** Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	N/A - Software GmbH is not a group health plan.
Organizational Safeguards	§164.314(b)(2) **Implementation specifications (Required).** The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—	N/A - Software GmbH is not a group health plan.
Organizational Safeguards	§164.314(b)(2)(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;	N/A - Software GmbH is not a group health plan.
Organizational Safeguards	§164.314(b)(2)(ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;	N/A - Software GmbH is not a group health plan.
Organizational Safeguards	§164.314(b)(2)(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and	N/A - Software GmbH is not a group health plan.
Organizational Safeguards	§164.314(b)(2)(iv) Report to the group health plan any security incident of which it becomes aware.	N/A - Software GmbH is not a group health plan.
Organizational Safeguards	§164.316 Policies and procedures and documentation requirements.	
Organizational Safeguards	§164.316 A covered entity or business associate must, in accordance with §164.306:	
Organizational Safeguards	§164.316(a) **Standard: Policies and procedures.** Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	CC 1.1 CC 1.1 CC 1.1 CC 1.3
Documentation Safeguards	§164.316(b)(1) **Standard: Documentation.**	
Documentation Safeguards	§164.316(b)(1)(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and	CC 1.1 CC 1.1 CC 1.3

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Documentation Safeguards	§164.316(b)(1)(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	CC 1.1 CC 1.1 CC 1.1 CC 1.1 CC 1.3
Documentation Safeguards	§164.316(b)(2) **Implementation specifications:**	
Documentation Safeguards	§164.316(b)(2)(i) **Time limit (Required).** Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	CC 6.5
Documentation Safeguards	§164.316(b)(2)(ii) **Availability (Required).** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	CC 1.1 CC 1.1 CC 1.3
Documentation Safeguards	§164.316(b)(2)(iii) **Updates (Required).** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	CC 1.3 CC 2.1