SOC 3 – SOC (Service Organization Controls) for Service Organizations:

Trust Services Criteria for General Use Report

Report on SAG Cloud GmbH's Description

of its

Alfabet Cloud System

Relevant to

Security and Availability

throughout the period of

April 1, 2019 to September 30, 2019

Aprio

Passionate for what's next™

Table of Contents

SECTION I..... 1

Independent Service Auditor's Report To the Management of SAG Cloud GmbH 2

SECTION II.....3

Management of SAG Cloud GmbH's Assertion regarding its Alfabet Cloud System 4

Management of SAG Cloud GmbH's Description of its Alfabet Cloud System 5

SECTION I

Independent Service Auditor's Report

Independent Service Auditor's Report
To the Management of SAG Cloud GmbH

Scope

We have examined SAG Cloud GmbH's (also known as SAG) assertion, that the controls within SAG's Alfabet Cloud System were suitably designed and operating effectively throughout the period of April 1, 2019 to September 30, 2019, to provide reasonable assurance that SAG's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (Applicable Trust Services) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). SAG's management is responsible for the suitability of design and the operating effectiveness of these controls of these controls. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of the system and the service organization's service commitments and system requirements; (2) assessing the risks that the controls were not suitably designed and/or were not operating effectively to achieve SAG's service commitments and system requirements, (3) performing procedures to obtain evidence about whether controls within the system were suitably designed and operating effectively to provide reasonable assurance that SAG's service commitments and system requirements were achieved based on the trust services criteria relevant to security; and (4) evaluating the overall presentation of description of the system boundaries.

Because of the nature and inherent limitations of controls, SAG's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, and failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes made to the system or controls, the failure to make needed changes to the system or controls or deterioration in the suitability of design and/or in the effectiveness of controls may alter the validity of such conclusions.

In our opinion, SAG's assertion that the controls within its Alfabet Cloud System were suitably designed and operating effectively throughout the period of April 1, 2019 to September 30, 2019, to provide reasonable assurance that SAG's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria, in all material respects.

Aprio, LLP

Atlanta, GA

December 5, 2019

SECTION II

Management Assertion and System Description

Management of Software AG's Assertion regarding its Alfabet Cloud System

Software AG is responsible for designing, implementing, operating, and maintaining effective controls over the Alfabet Cloud System throughout the period of April 1, 2019 to September 30, 2019, to provide reasonable assurance that Software AG's service commitments and system requirements relevant to Security and Availability were achieved.

We have performed an evaluation of the suitability of the design of the controls and their operating effectiveness throughout the period of April 1, 2019 to September 30, 2019, to provide reasonable assurance that Software AG's service commitments and system requirements were achieved based on the Trust Services Principles relevant to Security and Availability (applicable Trust Services Principle) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Software AG's objectives for the system in applying the applicable Trust Services Principle are embodied in its service commitments and system requirements relevant to the applicable Trust Services Principle.

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 of the system were suitably designed and operating effectively throughout the period of April 1, 2019 to September 30, 2019, to provide reasonable assurance that Software AG's service commitments and system requirements were achieved based on the applicable Trust Services Principle.

Gerd Schneider, Head of Cloud Security

Management of Software AG's Description of its Alfabet Cloud System

This document describes the standard cloud services descriptions managed by the Software AG Cloud Service Unit (CSU) supporting respective requirements of the Cloud Security Alliance (CSA) Consensus Assessment Initiative (CCM v3.0.1), ISO 27001:2013, 27017, 27018 and Trust Services criteria relevant to Security and Availability (applicable criteria) set forth in TSC Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, (AICPA Trust Services Criteria)*.

Software AG Overview

Software AG, an independent software company, enables enterprises to connect any technology—clouds, apps, devices and data—anywhere and any way they choose. More than Software as a Service, we're "Freedom as a Service," enabling faster innovation in an increasingly connected world. Trusted by top brands for 50 years, we'll never stop pioneering the future of data. More on our analyst-recognized software for the Internet of Things and self-service analytics, integration and APIs, and business transformation at softwareag.com.

Software AG's Principle Service Commitments and System Requirements

Software AG Cloud has designed and deployed an Information Security Management System (ISMS) based on the ISO/IEC 27001:2013 standard. Software AG standard Cloud services are in scope of the ISMS, and in addition, ARIS Cloud, Alfabet Cloud and webMethods Integration Cloud are in scope for regular SOC 2 Type II attestation reporting for security and availability.

Contractual commitments for service availability and recovery are defined in the respective Cloud service attachments and service specific descriptions.

The contractual aspects regarding data protection and privacy for the Data Controller (customer) and Processor (CSU) are provided via Data Processing agreements defined for the respective regions of the Cloud service and its respective contracts. This includes the Technical Organizational Measures which describe the data protection measures in alignment with the General Data Protection Regulation (GDPR).

Alfabet Cloud Services Specific Description

Alfabet helps organizations in making better IT investment decisions and reduce 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 enables 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 Cloud Enterprise

Dedicated IaaS using a single-tenant concept where customers dedicate resources encapsulated in a Virtual Network. Customer can select between several different geographical regions for hosting their tenant depending on best connectivity.

Alfabet Cloud FastLane

Alfabet FastLane is the latest SaaS solution for IT Portfolio Management from Software AG. The solution enables customers to navigate the complexity of IT portfolio management by turning unanswered questions into meaningful business insights. Alfabet FastLane is a pre-configured Cloud product, which is the simplest ITPM solution in terms of usability and understanding from Software AG. Alfabet FastLane allows customers to carry out enhanced decision-making, drive innovation and reduce time-to-market for portfolio planning. It creates operational efficiencies by eliminating information silos within organizations – thereby improving compliance to standard practices and reduces business and technical risk associated with IT Portfolio Management.

Components Relevant to Software AG Cloud Platform

Software AG Cloud is an open and independent Cloud platform. Its secure and reliable PaaS portal provides access to an ever-expanding set of integrated Cloud services. This platform supports a wide range of uses cases and is ideal for accelerating our customers digital transformation, social and mobile collaboration and infusing your Cloud projects with innovation.

- **IaaS Provider Infrastructure:** Key IaaS provider infrastructure service components and monitoring services supporting the delivery of Cloud services are described under Subservice Organizations.
- **Security and Monitoring Software**
- **Management Software**

People

Cloud Service Unit Information security roles and responsibilities

- CSU is compromised of the CSO and the Cloud Security, Compliance and Certification (CSCC) department.
- CSCC is a centralized unit which is responsible to initiate and control the implementation and operation of information security within CSU.
- CSO is a centralized unit, coordinating the activities related to service operations for Standard Cloud Services and includes the following key roles which are described in further detail in the Cloud ISMS A6 Organization of Information security:

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

Internal suppliers: CSU interacts with several other Software AG teams in order to provide the Standard Cloud services.

- **Research and Development (RnD):** RnD develops and releases new product versions twice 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 incidents are initially managed by a Global Support Customer Support Representative (CSR). If support cannot solve an

incident directly, the incident is escalated to either CSO for Cloud platform related issues, or to RnD for product related issues.

- **Product Management:** Product Management prioritizes new features for Software AG Cloud. They interface between RnD, CSO, Marketing and Sales for Cloud topics.
- **Global Information Service:** GIS provides IT services to CSU such as Communication, 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 CSO Team as a basis for delivering the service.

External Suppliers: IaaS providers services are described in subservice organizations.

Procedures

Standard procedures applicable to all standard Cloud services are described in the section below.

Customer Support: Standard Support for all Cloud products include a 24/7 access to the Customer web portal called Empower (https://empower.softwareag.com) where customers can search the Knowledge Center for articles, early warnings and technical whitepapers, access product documentation, and contact support through an eService interface. Within Empower, the customer can access all user guides, documentation, and application handbooks for the product, which are regularly updated with each release. Through the eService portal, customers can create incidents (support requests classified by crisis, critical or standard) and monitor the status of existing requests.

Contract Termination and Asset Removal: Upon expiry of the contract term, CSO will retain the latest state of the tenant including the latest tenant backup for 30 calendar days. CSO can provide Cloud customers with a backup of their customer data in the form of the last tenant backup – encrypted file. This tenant backup can be restored in each Cloud product specific installation.

All customer assets are securely deleted according to IaaS provider standards as outlined in Subservice Organizations. For dedicated Cloud services CSU will also terminate the IaaS provider management account and virtual infrastructure components used to host the Customer Tenant Data and temporary operational files. For shared Cloud services the customer tenant data and operational temporary files are securely destroyed during standard tenant offloading.

Procedures Review: All processes and procedures are regularly reviewed by CSO Management and relevant team members. A sample of recurring reviews are listed below.

- **Organizational Structure:** Including the assignment of roles and responsibilities and yearly review. Participants include the CSO team
- **Contract Changes:** Quarterly review is conducted in case of any amendments or service updates. Participants include the CSO team, CSCC, and Legal as necessary
- **Monitoring Process:** Reviewed on a yearly basis by the CSO Management and the Monitoring experts
- **Escalation Process:** Reviewed on a yearly basis by the CSO Management
- **Account Review:** Periodic review with CSO and CSCC Management

Data

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

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

Access to Tenant Data: Access control to the tenant application is in the responsibility of the customer. CSO personnel access to tenant data requires customer consent. In case of a support incident, which requires access to the customer's Cloud product tenant data, the customer can choose to grant access to the CSO to examine the issue by providing user credentials, function privileges and client license 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 (at rest). Processing of tenant content is directly encapsulated in the Cloud application accessed via the Cloud service. Only the Cloud Service Operations (CSO) and other authorized Software AG support groups have access to the IaaS hosted environments with least privileges and with two-factor authentication. All access attempts and activities within the hosted environments are logged using CSU monitoring and IaaS provider services. Physical security is in the responsibility of the IaaS provider as outlined in Subservice Organizations.

Classification of Information

Asset Classification Protection Levels: The asset classification levels are derived from the Risk Management Business Impact Criteria and from Security Requirements regarding Confidentiality, Integrity, and Availability of delivered services and related customer assets for Software AG Cloud customers.

Control Environments

CSU is a Software AG organizational unit providing Software AG standard Cloud services to its customers. CSU leverages some aspects of Software AG's overall control environment in the delivery of these services. The collective control environment encompasses management and employee efforts to establish and maintain an environment which supports the effectiveness of specific controls.

Integrity and Ethical Values: Software AG's conformance with the German Corporate Governance demonstrates that good corporate governance is a core component of management at Software AG. Software AG's Corporate Security Officer is responsible for awareness and complying with security policies, procedures and standards. In addition, every Software AG employee is required to comply with the Company's Code of Business Conduct and Ethics.

Management and Board of Directors: The Supervisory Board collaborates with the Software AG 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 decision of key relevance to Software AG. 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 were any deviations from planned business development is explained in detail.

Software AG Quality Management System: Software AG has implemented a quality management system (QMS) and is IS0 9001 certified for Global Support, Product Development & Management, and Global Consulting Services with GCS Sales and Managed Services - (worldwide) including supporting Services (IT Services, Human Resources, Facility Management and TA services). This is an independent validation of the Software AG quality system and determined that Software AG activities comply with ISO 9001 requirements. See also Software AG QMS certificate. Our QMS is foundational for assuring high customer satisfaction, delivering the best-quality support services and software as well as making continuous improvements. As part of our QMS, Product Development's and Global Support's system describes the processes, roles and rules that guide the daily work of every employee and how critical assets are secured. This framework:

Software AG Business Continuity Management System: Software AG has designed, deployed and maintains an ISO 22301 based Business Continuity Management System (BCMS) for the CSU business unit (as well as several other aspects of the Software AG enterprise.) Software AG achieved certification for this standard - IS 22301 Business Continuity Management System Certificate. The scope of the Software AG Business Continuity plan includes the functions of Support, Facility Management, Research and Development, IT-Services, Human Resources, Corporate Communications and Cloud Operations.

This BCMS program encompasses and enhances the security and availability related considerations represented by SOC 2 Trust Services Principles represented herein. Software AG CSU primary objectives for the BCMS include:

- Ensuring that the company's services and systems are available to meet its customers as committed and needed
- Proactive identification of threats and risks that could impair the continuity of CSU services, and as appropriate, timely responses to incidents
- Compliance with legal, regulatory and contractual requirements
- Governance structure to provide management timely and complete information to monitor the effectiveness of the BCMS to meet CSU information risk management objectives

Software AG Cloud Service Unit (CSU) Information Security Management Program (ISMP)

The Cloud Information Security Management Program (ISMP) secures Software AG Cloud with the highest industry standards. The ISMP encompasses and enhances the security related considerations represented by SOC 2 Trust Services Principles as well as ISO 27001:2013, 27017 and ISO 27018 controls. Customers can find further details about the ISMP and independent assurance evidence of security controls on the Software AG website and in the Cloud Security and Compliance fact sheet.

Monitoring Controls: The Software AG CSU has designed, deployed and monitors their information security management system (ISMS) in accordance with the ISO 27001:2013 standard. CSU achieved certification for this standard effective December 27, 2017 and has deployed a monitoring and surveillance audit program to maintain this certification through December 27, 2020. ISO/IEC 27017 and ISO/IEC 27018 standards have been added to the 2019 certification scope.

The independent third-party auditors' assessment, which validates compliance with the ISO 27001:2013 standard, provides evidence that the CSU ISMS is comprehensive and in accordance with industry-leading best practices. The certification scope statement lists the standard Cloud services in scope of the ISO 27001 certification and ISO/IEC 27018, ISO/IEC 27017 standards.

Assignment of Authority and Responsibility: Key roles and responsibilities are assigned to individuals responsible for operating the Cloud services. Team members have both the skills and competencies to match their responsibilities and receive annual training to maintain these skills. Team members whose responsibilities involve technical roles have external accreditation. Job descriptions are reviewed and revised as necessary on a yearly basis.

Talent Management Policies and Practices: All CSO employees are required to regularly complete the Global Code of Business Conduct training and receive performance reviews on an annual basis. The CSO team and the RnD team also complete an annual Cloud security training course lead by the CSCC Team which is formally reviewed as part the ISMS Governance process.

Policies and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints, are published and available in the process documentation made available to all internal users via the documented incident process model. The CSO team reviews and updates Cloud services procedural documentation on a semi-annual basis or as needed with product update.

Risk Management: The CSU risk management program covers all risks potentially impacting the confidentiality, integrity, and/or availability of CSO Cloud services and customer data.

Risk Assessment: An organizational and information technology risk analysis is performed to enable CSU to establish information technology systems and organizations that provide the security that is required by law and is proportionate to risks. The analysis makes it possible to identify the security flaws of IT systems, as well as entities of implemented controls that are ineffective. Therefore, a mandatory information technology and organizational risk analysis is carried out for CSU IT systems and CSU Organization at least annually.

Control Activities

System Account Management

Only authorized Software AG Support teams such as RnD, Global Cloud Support, and CSO members have access to the IaaS provider administration console and the infrastructure of the Cloud service. This access is controlled through a Central Account Management policy where users are assigned roles depending on the requirements of their position. The administrators can only access the IaaS provider administration console using multi-factor-authentication. Within the IaaS provider these roles are governed by a shared Trust Policy, An IaaS provider document in which a definition of roles and responsibilities of all parties are documented. All activity within the IaaS provider is logged and monitored.

Data Transfer

The transfer of customer data outside the Cloud service environment must be customer approved and in accordance with Information Transfer Security Requirements of the Communication Security Policy. Neither CSU nor third party IaaS Supplier will transfer customers' tenant content from the data centers of the IaaS Supplier Region unless required to comply with the law or requests of governmental entities or instructed by customer, CSU will notify customer as applicable.

Cryptography

Tenant data coming to or leaving the Cloud environment is transmitted through encrypted protocols with up-to-date encryption ciphers. Data-at-rest managed by CSU is protected using IaaS provider encryption capabilities according to the Cryptographic Controls Policy. Administrative access to the IaaS provider console is provided via encrypted protocols with up-to-date encryption ciphers and access to the OS-level of hosted resources is implemented via SSH/RDP using individual key-pairs. Cryptographic controls are provided by our ISO 27001:2013 compliant IaaS Supplier's in compliance with all relevant agreements, legislation and regulations.

Data Backup and Recovery Management

Cloud customers expect that support services are always available to safeguard the continuity of their business systems. To ensure full support of Cloud products, a Business Continuity and Disaster Recovery (BC/DR) policy for Software AG Global Support (and supporting functions) according to ISO 22301 standards has been enacted.

Incident Management

After a support incident is created, it is assigned to a SAG Global Support representative. The CSR initially troubleshoots the issue and if they cannot resolve it, they will determine whether the incident is related to the standard a specific Cloud product or to a Cloud specific topic. If it is related to a Cloud specific topic, the CSR will ask via Pivotal for CSO support. CSO will try to fix the issue or escalate to a product specific Cloud RnD team for support. In both cases, the Global Support team will be updated via Pivotal. If RnD has to be involved in an incident, an iTrac issue is created and all details to the incident are exchanged via iTrac between Global Support or CSO and RnD. iTrac is the ticketing system used for all development and production changes for products and cloud environments.

Change Management

Software AG Cloud products update process ensures a smooth upgrade with minimal customer impact. All changes to production Cloud services, including software updates, application/product changes, and virtual infrastructure changes are planned, evaluated, tracked, implemented and verified based on an established change management process. Data Center level security solutions and a SIEM solution are in place to log and alert on any changes to the production environments.

Platform Monitoring

Monitoring Controls: Based on ISO/IEC 27001:2013, ISO/IEC27017 and ISO/IEC27018 CSO maintains and improve the security controls monitoring processes through verification, monitoring and assessing performance of controls against organizational policies and objectives, and reporting the results to management for review.

The CSU Security Controls review process calls for a check on all security controls and measures for their effectiveness and suitability for the Cloud environment. Furthermore, based on the records of these monitored areas, management will be providing with evidence of verification and traceability of corrective, preventive and improvement actions regarding security controls. In addition, an annual review of controls is performed and ineffective controls as well as invalid controls are removed, while improved and new controls may be implemented. The CSO and CSCC management is involved in the review process and approves the final control matrix and the performance of each control.

Monitoring Procedures: The IaaS provider maintains responsibility for monitoring the IaaS infrastructure used by Software AG, while CSO is responsible for monitoring activity and usage within the boundary of Software AG's Cloud environment using audit logs, logging analysis and alerting tools, and data visualization tools.
Data points from system components and endpoints allow CSO to monitor system performance, potential security threats and vulnerabilities, resource utilization, and detection of unusual system activity. The CSO team receives alerts when the log data triggers certain performance metrics (such as an instance is not responding), a capacity warning or a latency issue. Depending on the severity of the alert, the responsible team member will review and make the necessary remediation.
The CSO team also proactively identifies system improvements using IaaS provider tools and additional third-party tools listed in Software, which provide optimization and best practice recommendations. This information is provided to support teams such as Product Management or RnD for enhancements.
Within the Cloud infrastructure, all servers are equipped with the infrastructure protection tool “Trend Micro Deep Security” that provides anti-virus protection, network intrusion detection and prevention, and integrity monitoring. Along with selected IaaS provider tools TrendMicro is used to alert the CSO team for proactive ways to improve security through network hardening and patching. It also identifies potential security incidents. Cloud System Administrators review Security logs and virus scan alerts on a weekly basis. Also, Administrators review weekly security status reports from these third-party tools and address them in the regular Product Change Advisory sessions as needed. The IaaS provider provides vulnerability scanning and base OS patching services as part of their general practices relating to their infrastructure. Any issues noted that could affect any IaaS provider customers, such as Software AG, are reported to them.
Service Monitoring Customer Capabilities: Customers can monitor Cloud Services availability via the Software AG Cloud Trust Site. Customers can access application logs via the specific interface of the Cloud application. Additional Information about service configuration and monitoring is available in the respective product documentation.

Security Testing

Security in Development: Software AG Cloud Products have a rigorous software design and development processes. RnD follows industry standards such as OpenSAMM for Software Development Lifecycle Management. RnD performs design review to verify the built-in security features and to identify any missing security features. The security team performs scans on third-party component to identify any vulnerabilities. In addition, manual penetration tests, log analysis, session mismanagement, platform specific attacks, etc., are performed on all the interfaces provided by the application. Any vulnerability noted is incorporated into the risk assessment process.

- **Security Static Analysis:** Source code is scanned using a static code analysis tool. Security experts perform the review before every release cycle of the Cloud products.
- **Security Dynamic Analysis:** The process involves per release application testing using the Software AG Cloud web interface just as an external attacker would do without the code access. Dynamic scanning tools are used that assist in identifying a wide variety of vulnerabilities, which primarily include:
    - Input/output validation such as cross-site scripting, and SQL injection;
    - Specific application problems
    - OWASP and CWE vulnerabilities;

Security Penetration Testing

For all the Cloud hosted products the Software AG RnD security team performs security penetration testing based on OWASP top 10 for each Cloud release.

In addition, Cloud Security, Compliance and Certifications engages with an external security testing company to perform regular penetration test for standard Cloud services. Customers can request latest summary test results and remediation plans to plan their respective vulnerability management process accordingly.

Subservice Organization – Amazon Web Services

AWS Services Description Overview

CSU Cloud Services are based upon infrastructure services provided by AWS and an installation of Software AG's respective standard products. Software AG has a strategic partnership with Amazon Web Services (AWS). Software AG is an All-In Technology Partner of AWS and benefits from the AWS Well-Architected Program.

AWS Supplier Management

A clear definition of roles and responsibilities for Software AG and AWS provides Software AG customers the needed transparency and trust that their services and data, systems, and applications are highly secure and available.

Software AG Responsibilities: CSU is responsible for the software components placed on the Cloud; the management (including updates and security patches) of the guest operating system; the configuration of the AWS provided security group firewall and other security-related features. CSU complies to the AWS Acceptable use policy.

AWS Responsibilities: AWS operates, manages and controls the components of the host operating system from virtualization layer down to physical security of the facilities where the AWS services operate. AWS is responsible for all physical access controls to IaaS for Software AG Cloud Services:

Applicable AWS Services

Infrastructure Services

- **AWS VPC:** A Virtual Private Cloud (VPC) service instance from AWS secures the customer's service installation against intrusion. Amazon VPC (Virtual Private Cloud) is used to provide a private, isolated section of the AWS Cloud where AWS resources are launched in a defined virtual network. See http://aws.amazon.com/vpc/
- **AWS EC2:** Amazon EC2 provides resizable compute capacity in the Cloud. EC2 (Elastic Cloud Compute) is the virtual computing environment with the Operating System. It is used for the deployment of the Cloud software and workloads of web application, application server and additional Cloud components. See http://aws.amazon.com/ec2/
- **AWS S3:** Amazon S3 (Simple Storage Service) provides a fully redundant data storage infrastructure. The AWS S3 instance is used to securely store all log information, for example the event monitoring and application log information etc. See http://aws.amazon.com/s3/
- **AWS ROUTE 53:** Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service, which is used for accelerated content delivery of the Cloud to remotely locate users by setting up a dedicated domain name for the customer. See http://aws.amazon.com/route53/
- **AWS Relational Database Service:** Amazon Relational Database Service (RDS) is used to set up, operate, and scale a SQL Server database in the Cloud. It provides cost-efficient and resizable capacity while managing time-consuming database administration tasks. See https://aws.amazon.com/rds/

- **AWS Elastic File System:** Amazon Elastic File System (EFS) provides a simple, scalable, elastic file system for Linux-based workloads for use with AWS Cloud services. See https://aws.amazon.com/efs/
- **AWS Directory Service:** AWS Directory Service is a managed service that is used to connect the Cloud end users with an existing on-premise Microsoft Active Directory at customer location. See https://aws.amazon.com/directoryservice/
- **AWS Identity & Access Management:** AWS Identity and Access Management (IAM) is used to securely control access to AWS services and resources for dedicated members of the Operations team including the AWS Directory Services in which they are entitled. See https://aws.amazon.com/iam/
- **AWS Key Management Service (KMS):** AWS Key Management Service is a managed service that enables users to create and control the encryption keys used to encrypt data and uses Hardware Security Modules to protect the security of keys. AWS Key Management Service is integrated with several other AWS services to help in protecting the data stored with these services. AWS Key Management Service is also integrated with AWS CloudTrail to provide users with logs of all key usage to help meet users' regulatory and compliance needs. See http://aws.amazon.com/kms/
- **AWS Lambda:** AWS Lambda allows users to run code without provisioning or managing servers. See http://aws.amazon.com/lambda/
- **AWS Simple Email Service (SES):** Amazon SES (Simple Email Service) is a highly scalable and cost-effective bulk and transactional email-sending service for the Cloud. It is used to configure the SMTP service related to the Alfabet software and for notifications to the Alfabet CSO Team related to the AWS Lambda configuration. See http://aws.amazon.com/ses/
- **Amazon Simple Queue Service (SQS):** Amazon Simple Queue Service is a fast, reliable, scalable, fully managed message queuing service. See http://aws.amazon.com/sqs/
- **AWS Simple Notification Service (SNS):** Amazon Simple Notification Service is a fast, flexible, fully managed push notification service that allow users to send individual messages or to fan-out messages to large numbers of recipients. Amazon SNS makes it simple and cost effective to send push notifications to mobile device users, email recipients or even send messages to other distributed services. See http://aws.amazon.com/sns/

Security and Monitoring Services

- **AWS Config:** AWS Config is a fully managed service that provides users with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. See http://aws.amazon.com/config/
- **AWS Inspector:** AWS Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS See https://aws.amazon.com/inspector/
- **AWS Guard Duty:** Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to help protect our AWS accounts and workloads. See https://aws.amazon.com/guardduty/
- **AWS Trusted Advisor:** AWS Trusted Advisor helps in provisioning resources by following best practices. AWS Trusted provides a general overview of all related AWS resources regarding Cost Optimizing, Performance, Security, and Fault Tolerance. See https://aws.amazon.com/premiumsupport/trustedadvisor/
- **AWS CloudTrail:** The AWS CloudTrail web service records AWS API calls and delivers log files. These log files are being stored in the S3 instance. See http://aws.amazon.com/cloudtrail/

- **AWS CloudWatch:** Amazon CloudWatch provides monitoring for AWS Cloud resources. Respective log files are stored in the S3 instance. See http://aws.amazon.com/cloudwatch/
- **AWS System Manager:** Amazon System Manager provides visibility and control of the AWS IaaS infrastructure. It provides a unified user interface to view operational data from multiple AWS services and allows automation of operational tasks across AWS resources. See https://aws.amazon.com/systems-manager/