SAG CLOUD GMBH

webMethods Cloud Services

SOC 3® System and System and Organization Controls (SOC) for Service Organizations Report throughout the period of April 1, 2020 through September 30, 2020

Report of Independent Service Auditor issued by Aprio LLP

Table of Contents

I. Report of Independent Service Auditor

To: Management of Software AG

Scope

We have examined Software AG's (the "Company") accompanying assertion that the controls within Software AG's webMethods Cloud Services ("description") were effective throughout the period April 1, 2020 to September 30, 2020 (the "Specified Period"), to provide reasonable assurance that Software AG'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 (AICPA, Trust Services Criteria).

Software AG uses Amazon Web Services and Microsoft Azure as subservice providers for hosting of the production infrastructure system and associated physical security and infrastructure support. The Assertion indicates that certain AICPA Applicable Trust Services Criteria specified in the section titled Software AG's Description of the Boundaries of its webMethods Cloud Services 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. Our examination did not extend to the controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Assertion indicates that certain AICPA Applicable Trust Services Criteria specified in the section titled Software AG's Description of its webMethods Cloud Services System, under the section User Entity Controls, can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service organization's responsibilities

Software AG 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. Software AG has provided the accompanying assertion titled Software AG's *Assertion* ("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 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. 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.

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
- 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;

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. 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

Opinion

In our opinion, SoftwareAG’s assertion that the controls within the webMethods Cloud Services 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, in all material respects, is fairly stated.

Aprio, LLP

Atlanta, Georgia
January 15, 2021

The SOC Logo is a proprietary trademark and service mark of the American Institute of Certified Public Accountants, which reserves all rights.

II. Software AG's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over the Software AG's (the "Company") webMethods Cloud Services (the "System") titled *Software AG's Description of its webMethods Cloud Services* throughout the period April 1, 2020 to September 30, 2020 (the "Specified Period"), to provide reasonable assurance that the Company's service commitments and system requirements relevant to Security, and Availability were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

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* (AICPA, *Trust Services Criteria*).

The Company's objectives for the system in applying the Applicable Trust Services Criteria are embodied in its service commitments and system requirements relevant to the Applicable Trust Services Criteria. The principal service commitments and system requirements related to the Applicable Trust Services Criteria are specified in Section III titled *Software AG's Description of its webMethods Cloud Services System*.

Software AG uses Amazon Web Services and Microsoft Azure as a subservice provider for hosting of the production infrastructure system and associated physical security and infrastructure support. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Software AG, to achieve Software AG's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Software AG's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Software AG's controls. The description does not disclose the actual controls at the subservice organization.

Certain AICPA Applicable Trust Services Criteria, specified in Section III, *Software AG's Description of its webMethods Cloud Services System* under the section User Entity Controls can be achieved only if complementary user entity controls contemplated 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 User Entities.

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 ahieve 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.

III. Management of Software AG's Description of its webMethods Cloud Services System

A. Scope and Purpose of the Report

This report describes the control structure of Software AG (the "Company") as it relates to its webMethods Cloud Services (the "System") for the period of April 1, 2020 to September 30, 2020 (the "Specified Period") for the Security and Availability Trust Services Categories (the "Applicable Trust Services Criteria") as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services 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 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.

C. Principal Service Commitments and System Requirements

Software AG Cloud uses an Information Security Management System (ISMS) based on the ISO/IEC 27001 standard and ISO/IEC 27017, ISO/IEC 27018 additional requirements. Software AG standard cloud services are in scope of the ISMS and in addition ARIS Cloud, Alfabet Cloud and webMethods 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 order forms and service specific descriptions.

The contractual aspects in regards to data protection and privacy for the data controller (customer) and processor (CloudOps) 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).

D. Components of the System Used to Provide the Services

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.

Software AG Cloud Information security roles and responsibilities

Cloud Security, Compliance and Certification (CSCC) is a centralized unit which is responsible to initiate and control the implementation and operation of information security within the Software AG Cloud Organization.

Cloud Operations (CLOUDOPS) is a centralized unit, coordinating the activities related to service operations for Standard Cloud Services and includes the following key roles:

- **Head of Cloud Services Operations:** 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. Ultimate point of escalation for product specific cloud operations issues.
    - Infrastructure: Manages Cloud Infrastructure as a Service (Iaas) 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:** The Cloud Operations Engineer is a supporting role for various cloud service 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 AG offices in Germany, Bulgaria, USA, , Malaysia and India. CLOUDOPS 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.

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.

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

Internal suppliers: CloudOps 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 CLOUDOPS 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, CLOUDOPS, Marketing and Sales for Cloud topics.
- **Global Information Service (GIS):** GIS provides IT services to Cloud Organization 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 (CM&L):** The CM&L Team is responsible for handover of a new contract to the CLOUDOPS Team as a basis for delivering the service

Data Privacy and protection: Aligned with GDPR requirements and as documented in the Privacy Policy for Standard & Managed Cloud Services the Software AG Data Privacy Office (dataprotection@softwareag.com) is the contact for customers and authorities in regards to 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 user name and password. 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. Customer is responsible for all activities that occur under its Account.

Access to Tenant Data: Access control to the tenant application is in the responsibility of the customer. CLOUDOPS 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 CLOUDOPS 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 CloudOps 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 CloudOps monitoring and IaaS provider services. Physical security is in the responsibility of the IaaS provider as outlined in Subservice Organizations.

Policies and Procedures: Standard procedures applicable to all standard cloud services are described in the section below. Procedures specific to a cloud service are described in the respective Cloud Services Specific Descriptions.

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, CLOUDOPS will retain the latest state of the tenant including the latest tenant backup for 30 calendar days. CLOUDOPS 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.

Software AG Cloud customers may request a list of all assets and document the schedule for the termination of service followed by the agreed time frame of their deletion. Assets of the Software AG Cloud customers that reside on the Software AG standard Cloud Service environments are removed, and returned upon termination according to the terms specified in the Cloud Services Order Form. No copies of Software AG Cloud customer's information will remain on the Software AG premises except any that may be required by local legislation rules.

All customer assets are securely deleted according to IaaS provider standards as outlined in Subservice Organizations. For dedicated cloud services CloudOps 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 CLOUDOPS 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 CLOUDOPS team.
- **Contract Changes –** Quarterly review is conducted in case of any amendments or service updates. Participants include the CLOUDOPS team, CSCC, and Legal as necessary.
- **Monitoring Process -** Reviewed on a yearly basis by the CLOUDOPS Management and the Monitoring experts.
- **Escalation Process -** Reviewed on a yearly basis by the CLOUDOPS Management.
- **Account Review -** Periodic review with CLOUDOPS and CSCC Management.

Control Environment: CloudOps is a Software AG organizational unit providing Software AG standard cloud services to its customers. CloudOps 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 Information 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. Cloud Organization Management ensures that all Cloud employees complete periodic security and compliance training.

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 (ITServices, Human Resources, Facility Management and TA services). This is an independent validation of the Software AG quality management system and determined that Software AG activities comply with ISO 9001 requirements.

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:

- Assures compliance with laws and regulations on quality, safety and performance
- Safeguards our ability to support our customers
- Clearly defines transparent processes
- Enables a continuous stream of innovation in an agile development environment
- Builds in feedback to assure we supply quality software that creates a competitive advantage for our customers

Software AG Business Continuity Management System: Software AG has designed, deployed and maintains an ISO 22301 based Business Continuity Management System (BCMS) for Global Support and CloudOps unit as a supporting function (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 is set as follows: Global Support (worldwide), including supporting services (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 CloudOps 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 Software AG Cloud 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 Software AG information risk management objectives.

Software AG Cloud Organization 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, 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 Cloud Organization has designed, deployed and monitors their cloud information security management system (ISMS) in accordance with the ISO/IEC 27001:2013 standard. Software AG Cloud Organization achieved certification for this standard effective December 27, 2017 and has deployed 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 certification scope in 2019.

The Cloud ISMS defines our approach to managing security for cloud services in a holistic, comprehensive manner and provides a suite of information security measures to:

- Protect cloud information assets from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction
- Proactively identify security risks, prevent, detect and respond to security breaches and violations
- Comply with legal, regulatory and contractual requirements
- Adopt an overarching management process to ensure information security controls meet information security needs on an ongoing basis

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

General requirements for security controls performance evaluation, including monitoring, internal audits and management reviews are described in the Cloud Information Security Policy (CISP). The CISP provides documented evidence of Cloud Organization implementation of information security controls can be provided to customers on request.

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 CLOUDOPS employees are required to regularly complete the Global Code of Business Conduct training, and receive performance reviews on an annual basis. The CLOUDOPS 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.*n*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 CLOUDOPS team reviews and updates Cloud Services procedural documentation on a semi-annual basis or as needed with product update.

System Descriptions and procedure documents are developed and verified by the CLOUDOPS team to document the design and operation of the system which is used to deliver the Standard Cloud Services. These documents are made available via the intranet to those personnel that need them to perform their job.

An annual performance assessment is performed by management for all CLOUDOPS team members to evaluate job performance versus expectations. In addition, personnel responsible for implementing, operating, maintaining, and monitoring of the system affecting security and availability complete formal training on an annual basis.

Organizational charts and procedural documents are in place to communicate key areas of authority, responsibility and lines of reporting to personnel responsible for the design, development, implementation, operation, monitoring, and maintenance of the system enabling it to meet the commitments and requirements as they relate to security and availability.

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

Risk Assessment: An organizational and information technology risk analysis is performed to enable the Software AG Cloud Organization 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 CloudOps IT systems and Cloud Organization at least annually.

A risk assessment is further performed in cases where an enhanced or priority new system, system component or application is deployed, the major version of an existing system or application is changed, or wherever appropriate due to negative external or internal effects.

This systematic approach to information security risk management is used to identify organizational needs regarding information security requirements and to create an effective Information Security Management System.

Risk Treatment: Risk treatment options are selected based on the outcome of the risk assessment, the expected cost for implementing these options and the expected benefits from these options. Each major risk (High probability and/or high impact) are assigned to a risk owner for monitoring and controlling purposes to ensure that the risk will not “fall through the cracks”.

Review of the Analysis: In the areas affected by actions to reduce risk, the analyses are reviewed at least annually, and any changes or modifications are documented.

Risk Communication and Consulting: To ensure correct risk handling is applied in all phases of the risk management process, all respective stakeholders must be involved.

Risk monitoring and Review: The monitoring and review of the risk management process is not bound to any fixed cycle, but is an integral part of all processes in the Cloud Organization. Risks will be assigned to the Cloud Risk Manager who tracks, monitors, controls and reports on the status and effectiveness of each risk response action to the Risk Management Program Owner and the Cloud Risk Owner.

Control Activities

System Account Management: Only authorized Software AG Support teams such as RnD, Global Cloud Support, and CLOUDOPS members have access to the IaaS provider administration console and the infrastructure of the Cloud services. 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 activities within the IaaS provider is logged and monitored.

Physical access to Software AG's operations facilities is strictly controlled and monitored via Software AG's Physical Access Security Policy. Software AG has implemented a quality management system and is IS0 9001 certified for Global Support and Research & Development, including supporting services (IT-Services, HR, Facility Management, and Global Consulting Services).

Based on the job requirements of the administrators, access rights are reviewed on an annual basis. Access is revoked from all production systems within 24 hours if a team member is terminated or positions are changed.

The CLOUDOPS and RnD teams follow enterprise standards regarding identity and access management in alignment with the Access Control Policy as follows:

- The use of generic and shared accounts is prohibited on the network, production applications, associated production databases, and associated infrastructure unless authorized by management,
- The Change Advisory Board reviews the assignment of system users to the accounts monthly,
- Any identified discrepancies are reported to management for corrective action.

Data Transfer: 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 SAG Cloud 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, CloudOps will notify customer as applicable.

Cryptography: Tenant data coming to or leaving from the cloud environment is is transmitted through encrypted protocols with up-to-date encryption ciphers. Data-at-rest managed by CloudOps is protected using IaaS provider encryption capabilities according to the Cryptogr aphic 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 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 available at all times 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 23001 standards has been enacted.

Like any other cloud platform, Cloud Products are exposed to potential risks that could disrupt business functions. The strategy for continuing business in the event of a major incident is to ensure the safety and security of employees; and to continue business functions and services from predefined alternative sites or restore business functions within the agreed upon SLA, RTO, and RPO. The BC/DR plan is tested and reviewed annually.

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 CLOUDOPS support. CLOUDOPS 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 CLOUDOPS and RnD. iTrac is the ticketing system used for all development and production changes for products and cloud environments.

In addition to submitting support incidents in Empower, customers may submit suggestions or product enhancements via Brainstorm or product specific tool as described in cloud services specific description. This tool will alert the Product Management team of the customer's request and permit the team to determine if it is an issue or valid opportunity for a product enhancement. If Product Management team determines that it is an issue, then it will be routed to the proper RnD or CLOUDOPS team and will be managed in the iTrac ticket system.

When submitting Security Incidents to Software AG Global Support, Customer must indicate this aspect to the support representative or set the security flag in the support ticket if reported via custnmer support portal. For incidents that are a level 1 or 2 in severity (customer data is exposed, system cannot be used, threat of repetition of attack), an iTrac Alert type ticket is created. The Head of CLOUDOPS and the Security Team review and determine appropriate steps. For Severity 1 incidents, the customer(s) will be notified within 4 hours of discovery. For Severity 2 incidents, the customer(s) will be notified within 24 hours of discovery. The notification method for Cloud Enterprise customers is through an incident ticket in Empower which generates a direct e- mail. The notification method for the public Cloud environment is through a Security Alert on Empower. Customers can subscribe to all alerts per product for direct email notification.

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.

The steps for a product change are documented and tracked in a tracking tool (iTrac). The tracking tool is used to document the changes, any anomalies, and to log a pass or fail status for each phase of the change. As part of the Change Management process, every phase (development, test, and QA) of the change must receive a pass status before the next phase in the change can be started. Version control software is also incorporated as part of the lifecycle process. This ensures no issues or disruptions take place when a scheduled change is migrated into the production environment. In addition, security testing is performed prior to a change release.

The same Change Management Lifecycle process is used to address required changes around deficiencies or issues discovered by the users. All changes of this type go through a review board process, be accompanied by a detailed test plan, documentation of changes, implementation plan, risk mitigation plan, production manager approval, and user approval/agreement before the change is migrated to the user’s production environment.

Customers are provided with the releases notes through the Empower portal. Planned Maintenance windows are available at the Software AG Cloud Trust Site and announcements of new cloud releases are available in Empower.

Platform Monitoring

Monitoring Controls: Based on ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018, Software AG maintains and improves 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 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. CLOUDOPS and CSCC management is involved in the review process and approves the final control matrix and the performance of each control. General requirements for security controls performance evaluation, including monitoring, internal audits and management reviews are described in the Cloud Information Security Policy.

Monitoring Procedures: The IaaS provider maintains responsibility for monitoring the IaaS infrastructure used by Software AG, while CLOUDOPS is responsible for monitoring activity and usage within the boundary of Software AG's cloud environment through the use of audit logs, logging analysis and alerting tools, and data visualization tools. CLOUDOPS configures Network Time Protocol (NTP) on all IaaS provider instances, and the systems time is synchronized with a load-balanced pool of public servers on the Internet. These data points from system components and endpoints allow CLOUDOPS to monitor system performance, potential security threats and vulnerabilities, resource utilization, and detection of unusual system activity. The CLOUDOPS 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. If the actions involve the production architecture or the RnD product team, an iTrac ticket is created to document the remediation steps.

All logs of system activity are stored for at least 90 days and are protected from loss, destruction, falsification, unauthorized access and unauthorized release as described in accordance with legislatory, regulatory, contractual and business requirements.

The CLOUDOPS 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 CLOUDOPS 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 the Software AG Cloud Trust Site. Customers can access applications 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 vulnerabilities;
- 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.

webMethods Cloud Services Specific Description

webMethods Cloud provides foundation services to the Software AG Cloud platform as well as specific webMethods cloud services functionality.

webMethods API Cloud

Software AG's webMethods API Cloud is an API Management-as-a-Service platform that makes it easy to securely manage and expose APIs to your developer and partner community. The platform includes webMethods API Cloud Portal and webMethods API Cloud Gateway.

Components Relevant to API Cloud Platform

API Gateway: When you expose your APIs to the world, security is your top priority. API Cloud's gateway protects you from unauthorized and malicious users, while also giving you full control and visibility over who's accessing your APIs. API Gateway Cloud is a collection of many components. Except very few common components like load- balancer, the resources are dedicated because being a runtime, load from one customer might influence performance of the other. Customer can select between several different geographical regions for hosting their tenant depending on best connectivity.

API Portal: This is the place where developers discover and try your APIs. The developer portal is the public face of your API offerings and enables you to create and grow your ecosystem.

API portal is multi-tenant where customers share resources in a Virtual Private Cloud. Customer can select between several different geographical regions for hosting their tenant depending on best connectivity.

API Cloud Procedures

Customer Onboarding: After an API Cloud opportunity is successfully closed, the Direct Sales team provides the customer contract to the Contract Admins. Then a Contract Admin creates a new contract in SAP and provides the contract information and customer license files to the Logistics team and CLOUDOPS team. At this point, customers are also provided the counter-signed Cloud Services Agreement (also known as the Master Service Agreement) which includes a security and availability exhibit, the SLAs, and product specifications for their reference.

API Gateway Onboarding: For API Gateway customers, Cloud Ops receives a ticket and executes the deployment for the new tenant. The customer receives an automated confirmation e-mail on completion which includes their access credentials.

API Portal Onboarding: The deployment process for API Gateway provisions API Portal for a new tenant if this is part of the request.

Service Level Reporting: As specified in the cloud contract order form service availability is 99.5%. For API Cloud, the customer can subscribe for notifications on the Software AG Cloud trust site https://trust.softwareag.com/

API Cloud Data

API Data Backup and Recovery Management: API Cloud Customers expect that support services are available at all times to safeguard the continuity of their business systems. To ensure full support of API Cloud Products, a Business Continuity and Disaster Recovery (BC/DR) policy for Software AG Global Support (and supporting functions) according to ISO 23001 standards has been enacted.

Like any other cloud platform, API Cloud Products are exposed to potential risks that could disrupt business functions. The strategy for continuing business in the event of a major incident is to ensure the safety and security of employees; and to continue business functions and services from predefined alternative sites or restore business functions within the agreed upon SLA, RTO, and RPO. As specified in the cloud order form the system provides a Recovery Point Objective of 24 hours and a Recovery Time Objective of 12 hours.

The BC/DR plan is tested and reviewed annually. For Cloud products, an automated backup process is established, tested and reviewed periodically. A backup of the API Cloud tenant is executed daily and contains all of the API customers' data. Backups can be restored in case of disaster as defined in the Master Service Agreement. For Business Continuity, API Cloud servers are mirrored in different AWS Availability zones within the defined Region. API Cloud installations are also redundant across different availability zones for failover.

webMethods.io Integration

webMethods.io Integration is Software AG's Integration Platform as a Service (iPaaS) offering which provides a combination of capabilities offered by ESBs, data integration systems, API management tools, and B2B gateways. It empowers organizations to easily integrate devices, on-premise systems, and Software-as-a-Service (SaaS) applications such as Salesforce and ServiceNow. With its robust and secure architecture coupled with a wide range of features, it helps enterprises boost agility and enhance their business process efficiency.

The following summarizes core features of webMethods.io Integration:

- Smart, intuitive user interface for creating complex integrations quickly and easily
- Sophisticated orchestration which ensures that all integrations can be created, managed, and monitored through a central location easily
- Seamless and secure integration of on-premise systems, devices, and over 250 SaaS applications
- In-house applications to facilitate file transfer, data mapping, and data transformation
- Support for creating custom applications that suit specific integration requirements
- Vast library of ready-to-use integrations which can be customized further based on business needs
- Multi-tenant architecture that caters to scaling requirements of all organizations - big and small
- Stages management support which enables to promote a project from development-testing- production stage
- End-to-end monitoring for finding and resolving performance issues faster

Core Features

- User Interface: webMethods.io Integration's user interface is built for developers as well as business users. The user interface supports wizards and embedded help links to guide users in integration creation process.
- Sophisticated Orchestration: webMethods.io Integration offers sophisticated orchestration to rapidly develop agile applications which can be managed and monitored from a central location.
- Wide Range of Supported Applications webMethods.io Integration provides out-of-the box connectivity to SaaS applications such as Salesforce, ServiceNow, and StrikeIron as well as industry standard protocols such as REST, SOAP, and OData. Apart from this, the in-house applications such as FTP/SFTP and Transform provide file transfer and data mapping and transformation capabilities. Additionally, webMethods.io Integration supports custom application development to allow creating tailor-made applications for specific integration needs.
- Mapping and Transformation: Connect multiple applications, map the data of one application with another, and transform the application data in a way that best suits your business requirements, all through a simple drag-and- drop interface which can be easily used by business users.

- Stage Management: webMethods.io Integration provides a default environment for each tenant. Tenant owners can register their other tenants as additional environments and use this multi-environment structure to manage their project development lifecycle. Tenant owners can create and configure integrations in one environment, and when ready, publish them to another environment for use. This segregates the development environment of your tenant from the production one, thereby eliminating any chances of outages usually caused while migrating data from development to production.
- End to-end Monitoring: webMethods.io Integration allows you to have clear visibility into all of your webMethods.io systems with a dynamic view of your webMethods.io service calls as they move through various runtimes in API, B2B and Integration. Find performance issues faster with Root Cause Analysis, which enables you to drill-down further into the runtime and pin point where the problems are.

webMethods.io Integration Cloud Procedures

Customer Onboarding: After a webMethods.io opportunity is successfully closed, the Direct Sales team provides the customer contract to the Contract Admins. Then a Contract Admin creates a new contract in SAP and provides the contract information and customer license files to the Logistics team, CSM and CLOUDOPS team. Customers are also provided with the counter-signed Cloud Services Agreement (also known as the Master Service Agreement) which includes a security and availability exhibit, the SLAs, and product specifications for their reference.

Logistics sends an initial welcome e-mail to customers containing the link to register a tenant on the webMethod s.io platform in the region selected. Customers are responsible for creating their initial tenant and returning the name of their sub-domain back to Software AG. Once the tenant is created, customers receive an automated e-mail. This e-mail contains all necessary information to access the webMethods.io tenant.

The Logistics team provides the selected sub-domain tenant name to CSM team. CSM team checks the registration data of customers and provisions the Customer tenant as per the agreement.

Service Level Reporting: As specified in the cloud contract order form service availability is 99.9%. Customers can subscribe for availability notifications on the Software AG Cloud trust site.
https://trust.softwareag.com/integrationcloud/status/

Data Backup and Recovery Management: The complete webmethods.io system is backed up on daily basis. The automated backup is of three data sources which includes mongo database, aws rds and git document repository. These objects contains all data from webmethods.io customers. Following are the backup policies for mentioned data sources,

- Mongo DB - Automated daily backup with point in time recovery via Mongo Cloud Manager along with automated daily backup to S3 with retention period of 30 days.
- AWS RDS - Automated daily snapshot backup with retention period of 30 days.
- Git Repository - Automated daily backup to S3 with retention period of 30 days.

This backup is intended to ensure that the entire system can be recovered. If a disaster tear-downs the existing infrastructure, a fresh installation of webmethods.io can be configured with new AWS environment. Post completion of webmethods.io installation, customer data can be recovered from above mentioned backups.

As specified in the cloud contract order form the system provides a Recovery Point Objective of 24 hours and a Recovery Time Objective of 12 hours.

E. User Entity Controls

The Software AG Cloud is designed with the assumption that certain controls will be implemented by customers (user entities). Such controls are called complementary user entity controls. It is not feasible for all of the control activities related to the Cloud Products to be solely achieved by Software AG. Accordingly, user entities should establish their own internal controls or procedures to complement those of Software AG. The cloud service customer is responsible to define or extend its existing policies and procedures in accordance with its use of Software AG cloud services, and make cloud service users aware of their roles and responsibilities in the use of the cloud service. Contractually agreed customer responsibilities in regards to information security and data privacy are stated in the Cloud Services Agreement. To provide additional assurance that the specified control activities described within this report are met, user entities are responsible for: :

- Establishing logical security controls to restrict and monitor access to cloud systems
- Immediately notifying Software AG of any actual or suspected information security breaches, including compromised user accounts
- Effectively restricting access rights to authorized personnel; including administrative privileges and those for end users who access the environment
- Effectively restricting access control to the tenant application and may grant CLOUDOPS personnel access providing user credentials, function privileges and client license to access the data
- Ensuring the confidentiality of any user accounts and passwords assigned to them for use with the cloud systems
- Ensuring that their data stays encrypted within their managed environments
- Compliance with all applicable laws, including without limitation all applicable export and import laws and regulations of such other countries, associated embargo and sanctions regulations and prohibitions on export for certain end uses or by any prohibited end users

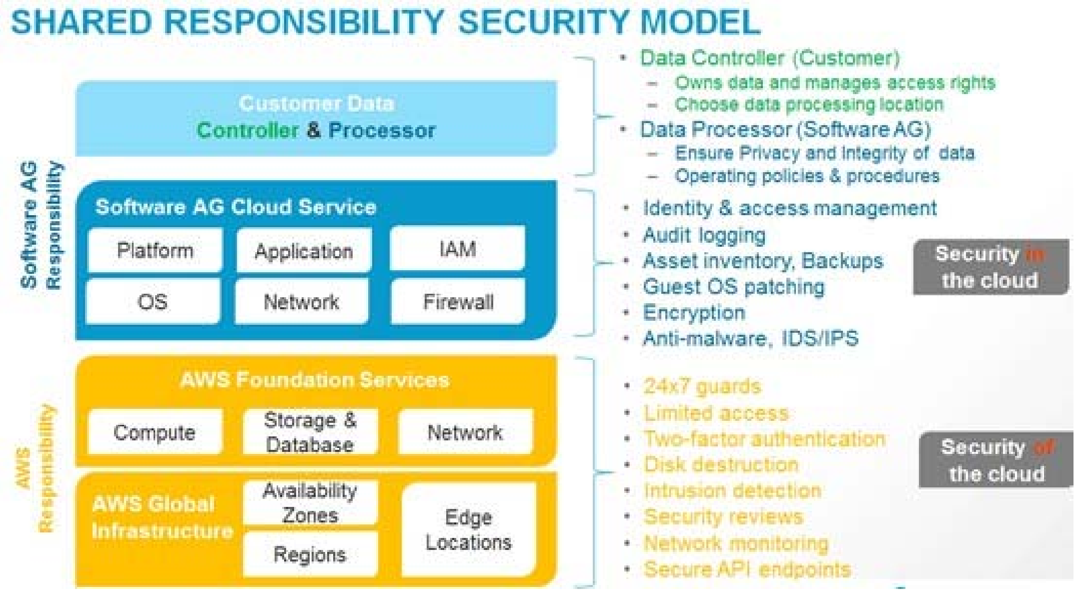
F. Subservice Organizations

Amazon Web Services

AWS Services Description Overview: SAG 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 and AWS share responsibility for operating the Software AG cloud infrastructure using AWS services as shown in the figure below.



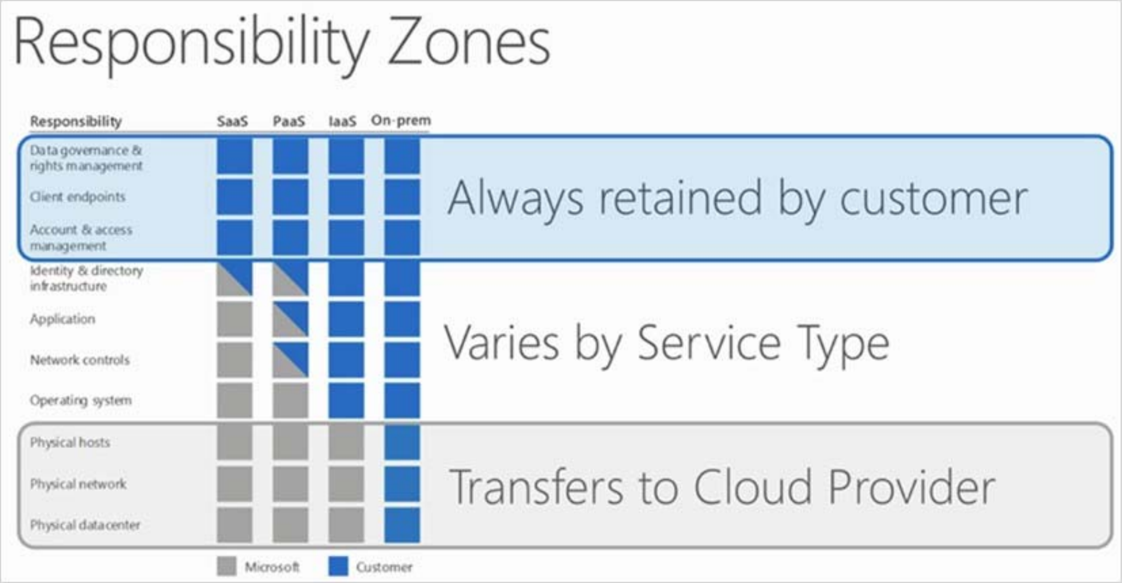
Software AG Responsibilities: SAG Cloud is responsible for the software components placed on the cloud; the management (including updates and security patches) of the guest operating system; the configuration of the AWS provided security group firewall and other security-related features. SAG Cloud Organization complies to the AWS Acceptable use policy. The Cloud Security, Certifications and Compliance team reviews reports and certificates including, but not limited to, SOC 2 reporting and ISO 27001 certificates, from independent parties for evidence that AWS is fulfilling their contractual obligations as documented in agreements with Cloud products. For more information, please see the following:

- AWS Cloud Compliance;
- AWS Risk and Compliance Whitepaper;
- AWS Security Whitepaper.

Microsoft Azure

Azure Service Description Overview: SAG Cloud Services are based upon infrastructure services provided by Microsoft Azure and an installation of Software AG's respective standard products.

Azure Supplier Management: Software AG has a strong partnership with Microsoft and is a long term Microsoft customer for Office Productivity Software. A clear definition of roles and responsibilities for Software AG and Microsoft Azure provides Software AG customers the needed transparency and trust that their services and data, systems, and applications are highly secure and available. The following responsibility matrix shows the areas of the stack in a software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) deployment that SAG Cloud (Customer) is responsible for and Microsoft is responsible for.



Software AG Responsibilities: SAG Cloud Organization 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 network configurations and other security-related features. The Cloud Security, Certifications and Compliance team reviews reports and certificates including, but not limited to, SOC 2 reporting and ISO 27001 certificates, from independent parties for evidence that Microsoft Azure is fulfilling their contractual obligations as documented in agreements with Cloud products. For more information, please review respective Microsoft documentations.

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

Software AG Cloud platform

SAG Cloud Services Specific Description: SAG Cloud is an umbrella product providing subscription to Software AG Cloud free trials. It provides a centralized entry point for subscribing to Software AG free-trials that are hosted on the Software AG cloud. Customers can subscribe through SAG Cloud for trials of Alfabet Fastlane, ARIS Cloud Advanced, Cumulocity IoT and WebMethods suite of products (Agile Apps cloud, WebMethods Integration Cloud , API Cloud). SAG Cloud is currently rolled out in Oregon (US West) and Frankfurt (EU) regions.

Components Relevant to the SAG Cloud Platform:_SAG Cloud is built to aid in easier self-service and a common entry point into product subscription for Software AG products in the cloud. In its essence, SAG Cloud is a thin wrapper that consists of a web interface and a tenant and identity management module that maintains the customer life-cycle and subscriptions (together with provisioning) to Software AG products described above (see SAG Cloud Services Specific Description)

Service Level Reporting:_As specified in the cloud contract order form service availability is 99.5%. The customer can subscribe for notifications on the Software AG Cloud trust site https://trust.softwareag.com/sagcloud/status/.

SAG Cloud Data:_ SAG Cloud is a supporting umbrella product that aids in the self-service of product registration and management of a product suite. As such, customer data is stored in the specific product that SAG Cloud offers access to. The KeyCloak database is a highly-scalable and multi-node distributed databases that is scaled over multiple regions and multiple shard farms, guaranteeing fast recovery in case of failure and duplication of the underlying data.

SAG Cloud Architecture: SAG Cloud consists of region-specific and global infrastructure.