SOFTWARE AG CLOUD

Cumulocity IoT Cloud System

System and Organization Controls (SOC) for Service Organizations Report
for the period of April 1, 2021 to September 30, 2021

Aprio
Passionate for what's next®

Report of Independent Service Auditors issued by Aprio LLP

Table of Contents

I. Report of Independent Service Auditor

We have examined Software AG Cloud's (the "Company" or "Software AG") accompanying assertion titled *Software AG Cloud's Assertion* (the "Assertion") that the controls within the Cumulocity IoT Cloud System (the "System') were effective throughout the period April 1, 2021 to September 30, 2021 (the "Specified Period") to provide reasonable assurance that Software AG Cloud'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*).

The Assertion notes that the Company uses Amazon Web Services (AWS) and Microsoft Azure, subservice organizations, for its third-party hosting of servers and equipment in an infrastructure-as-a-service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The Assertion indicates that certain AICPA Applicable Trust Services Criteria specified in the section titled *Software AG Cloud's Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Our examination did not extend to the controls of the subservice organizations, 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 Cloud's Description of the Boundaries of its 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

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *Software AG Cloud's Assertion* about the suitability of design and operating effectiveness of controls. When preparing its assertion, the Company is responsible for selecting, and identifying in its assertion, the Applicable Trust Services Criteria and 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 organizatin'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.

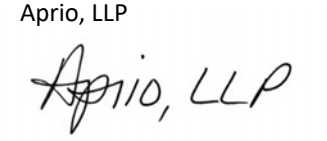
Other matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the section titled *Software AG Cloud's Description of the Boundaries of its System*, and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, Software AG Cloud's assertion that the controls within the Company's System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria, in all material respects, is fairly stated.

Aprio, LLP



Atlanta, Georgia
November 8, 2021

II. Company Name's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over Software AG Cloud's (the "Company" or "Software AG") Cumulocity IoT Cloud System (the "System") throughout the period April 1, 2021 to September 30, 2021 (the "Specified Period"), to provide reasonable assurance that the Company's service commitments and system requirements relevant to Security and Availability were achieved. We have performed an evaluation of the effectiveness of the controls within the system throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (the "Applicable Trust Services Criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (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 the section titled *Software AG Cloud's Description of the Boundaries of its System*.

Software AG Cloud uses Amazon Web Services (AWS) and Microsoft Azure, subservice organizations, for its third-party hosting of servers and equipment in an infrastructure-as-a-service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. Certain AICPA Applicable Trust Services Criteria specified in the section titled *Software AG Cloud's Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations.

Certain AICPA Applicable Trust Services Criteria, specified in Section III, *Software AG Cloud's* Description of the Boundaries of its 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 achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria.

III. Software AG Cloud's Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of Software AG Cloud (the "Company" or "Software AG") as it relates to its Cumulocity IoT Cloud System (the "System") for the period of April 1, 2021 to September 30, 2021 (the "Specified Period") for the trust services criteria relevant to Security and Availability (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

Company Overview

Software AG Cloud, 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, the Company never stops pioneering the future of data. More on the Company's analyst-recognized software for the Internet of Things and self-service analytics, integration and APIs, and business transformation can be found at softwareag.com.

C. System Overview

Software AG Cloud is an open and independent cloud platform. Its secure and reliable Platform-as-a-Service (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 its customers digital transformation, social and mobile collaboration–and infusing their cloud projects with innovation.

1. **Infrastructure-as-a-Service (IaaS) Provider Infrastructure**

   Key IaaS provider infrastructure service components and monitoring services supporting the delivery of Cloud services are described in Parts 9 and 10 of this section of the report.

2. **Software**

   Security and Monitoring Software

   Key components supporting the delivery of cloud services include:

   - *IaaS Provider:* The IaaS Provider(s) provides security and monitoring services as outlined in Parts 9 and 10 of this section of the report.
   - *Trend Micro "Deep Security":* Deep Security is an Infrastructure Protection tool that provides Intrusion Detection and Prevention, virus scanning, and vulnerabilities scanning for the customer's environment.

     See http://www.trendmicro.com/aws/

- *CrowdStrike:* CrowdStrike provides cloud workload and endpoint security, threat intelligence, and cyberattack response services.

  See https://www.crowdstrike.com/
- *DivvyCloud:* DivvyCloud monitors and assesses cloud and container environments for security misconfigurations, infrastructure weaknesses, and policy compliance violations.

  See https://divvycloud.com/
- *Splunk:* Splunk Enterprise helps enable the ability to search, monitor, and analyze machine data to gain valuable security monitoring intelligence and insights.

  See http://www.splunk.com/en_us/products/splunk-enterprise.html
- *Duo Security:* Duo's Trusted Access platform secures the Company by verifying the identity of its users and the health of their devices before they connect to the Company's applications.

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

  See https://www.okta.com/
- *JumpCloud:* JumpCloud® is a central source of authentication, authorization, and management of employees and their devices and the IT applications they access.

  See https://jumpcloud.com
- *Akamai:* Akamai provides Enterprise access management (EAA).

  See https://www.akamai.com
- *KeePassXC:* KeePassXC is a free open-source password manager which helps in managing passwords in a secure way. All passwords are kept in one database which is locked with one master key or a key file. The database is encrypted.

Management Software

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

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

  See https://www.atlassian.com/software/confluence
- *Jira (iTrac):* iTrac is the Cloud Service Operations (CloudOps) and RnD bug fix and change management ticketing system. Customer incidents can be escalated to iTrac from Pivotal by the Global Support team or directly entered as incidents are identified.

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

3. People

Cloud Service Unit Information security roles and responsibilities

Cloud Security, Compliance and Certification

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 function that defines all cloud operating functions of cloud family's business units and supportive cross-function cloud platform and cloud security and includes the following key roles which are described in further detail in the Cloud ISMS A6 Organization of Information security.

Head of BU Cloud Services

Responsible for team management, coordination of service delivery, and compliance with cloud policies. This role conducts procedure reviews and participates in regular advisory sessions for change management and risk assessment.

Cloud Operations System Owners

- Cloud Delivery: Provides cloud product specific team leadership and is responsible for day-to-day management and coordination of running the service. This role is the ultimate point of escalation for product specific cloud operations issues.
- Infrastructure: Manages Cloud IaaS Infrastructure operational relationships for respective providers and provides common services applicable to all cloud systems.
- Automation: Delivers Infrastructure-as-code and provides cloud service specific baseline.
- Security: Responsible for security oversight across all CloudOps cloud services.

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, Australia, Malaysia and India. CloudOps is distributed in different time zones to provide “follow the sun” coverage for customer’s support needs and to offer maintenance windows outside of customer’s standard business hours.

Management and Board of Directors

The Supervisory Board collaborates with the Software 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 where any deviations from planned business development is explained in detail.

External Suppliers

IaaS providers services are described in Parts 9 and 10 of this section of the report.

Internal suppliers

CloudOps interacts with several other Software AG teams 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 R&D 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.

- *IT:* The team provides IT services to CloudOps 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 CloudOps Team as a basis for delivering the service.

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

Access to Tenant Data: Access control to the tenant application is in the responsibility of the customer. CloudOps personnel's access to tenant data requires customer consent. In the 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 CloudOps to examine the issue by providing user credentials, function privileges and client license to access the data. All customer tenant data 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 data is directly encapsulated in the cloud application accessed via the cloud service.

Only 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 Parts 9 and 10 of this section of the report.

5. 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 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 in an 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 Cloud Services Order Form terms. No copies of Software AG Cloud customer's information are retained on the Software AG premises except any that local legislation rules may require.

All customer assets are securely deleted according to IaaS provider standards as outlined in Parts 9 and 10 of this section of the report. 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 dedicated cloud services. The customer tenant data and operational temporary files are securely destroyed during standard tenant offloading for shared cloud services.

Procedures review: CloudOps Management and relevant team members regularly review all processes and procedures. 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 the 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: The Software AG Cloud Organization provides Software AG standard cloud services to its customers. The Software AG Cloud Organization 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 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. Software AG Cloud Management helps ensure that all Cloud Operations 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 (IT Services, Human Resources, Facility Management and TA services). This certification is an independent validation of the Software AG quality system and verifies that Software AG activities comply with ISO 9001 requirements. Customers can reference the Software AG QMS certificate.

The Company's 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 the 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 Software AG's ability to support its customers
- Clearly defines transparent processes
- Enables a continuous stream of innovation in an agile development environment

- Builds in feedback to assure that Software AG supplies quality software that creates a competitive advantage for its 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 business unit as a supporting function (as well as several other aspects of the Software AG enterprise). Software AG has achieved certification for this standard as evidenced by the ISO 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, Global Communications and Cloud Operations).

This BCMS program encompasses and enhances the security and availability related considerations represented by SOC 2 Trust Services Criteria represented herein. The Software AG Cloud Organization's 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 Criteria 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 information security management system (ISMS) in accordance with the ISO 27001:2013, ISO/IEC 27017, and ISO/IEC 27018 standards. Software AG achieved certification for this standard effective on December 27, 2017 and has deployed a monitoring and surveillance audit program to maintain this certification through December 27, 2023.

The Cloud Organization ISMS defines the Company's 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; and
- 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 Organization ISMS is comprehensive and in accordance with industry-leading best practices. The certification scope statement lists the standard cloud services in scope of the current ISO/IEC 27001 (along with ISO/IEC 27018 and ISO/IEC 27017 requirements) certification 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 the Software AG Cloud Organization implementation of information security controls and 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 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 yearly.

Talent Management Policies and Practices: All CloudOps employees must complete the Global Code of Business Conduct training when changes are made and receive performance reviews annually. The CloudOps team and the RnD team also complete an annual cloud security training course lead by the CSCC Team, formally reviewed as part of the ISMS Governance process.

Policies and procedures documents for significant processes, including 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 updates.

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

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 Information Security 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 help 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 instances 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.

Risk management is performed according to the Software AG Cloud Organization’s risk management program which encompasses the following phases:

- Identify - These efforts identify technical and business risks to the organization and operations.
- Assess – The assessment phase evaluates the potential impact(s) of identified risks, the likelihood of occurrence, and control effectiveness and maturity.
- Mitigate – Mitigation develops risk treatment plans to control or reduce risk where needed, including the implementation of controls, processes, and other physical and virtual safeguards.
- Report – Reporting and communication is performed to help ensure that risk owners and stakeholders, as well as senior leadership, have visibility into risks to the organization and that there is effective decision making around risks.
- Monitor – Identified and assessed risks are periodically reviewed, along with any associated risk response efforts for the risk, to determine if their state or status has changed.

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".

One of the following approaches will be selected to manage assigned risks:

- Avoid – Eliminate the threat or condition or to protect the project objectives from its impact by eliminating the cause;
- Modify (Mitigate) – Identify ways to reduce the probability or the impact of the risk. Define actions to be taken in response to risks;
- Retain (Accept) – The remaining tread and thus the resulting risk are accepted by the management and management is accountable for the consequences; and
- Transfer – Shift the consequence of a risk to a third party together with ownership of the response by making another party responsible for the risk (buy insurance, outsourcing, etc.).

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: All respective stakeholders must be involved to help ensure correct risk handling is applied in all phases of the risk management process.

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 CloudOps. 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.

6. 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 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.

Physical access to Software AG's operations facilities is strictly controlled and monitored via Software AG's Physical Access Standard. 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, and
- 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 CloudOps nor a 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 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 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 Software AG's 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 help 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 help 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 Software AG Security Operations Center representative. The SOC classifies the issue, they will determine whether the incident requires the establishment of a Security Incident Response Team according to the specific classification. 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 the customer facing ticketing system, customers may submit suggestions or product enhancements via Brainstorm or product specific tools 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 the 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.

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 Incident Manager and the Security Incident Response Team review and determine appropriate steps. For Severity 1 incidents, the customer(s) will be notified within four 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. The notification method for the public Cloud environment is through a Security Alert. Customers can subscribe to all alerts per product for direct email notification.

Change Management: Software AG Cloud Products update processes help ensure 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 process helps ensure that 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, are 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.

7. Platform Monitoring

Monitoring Controls: Based on ISO/IEC 27001, ISO/IEC27017 and ISO/IEC27018, CloudOps 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 provides 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 perform 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 legislative, regulatory, contractual, and business requirements.

The CloudOps team also proactively identifies system improvements using IaaS provider tools and additional third- party tools listed in the Software section of this Report, 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 to proactive ways to improve security through network hardening and patching. The tool 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 applications logs via the specific interface of the cloud application. Additional Information about service configuration and monitoring is available in the respective product documentation.

8. 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 reviews 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 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 of 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 the latest summary test results and remediation plans to plan their respective vulnerability management process accordingly.

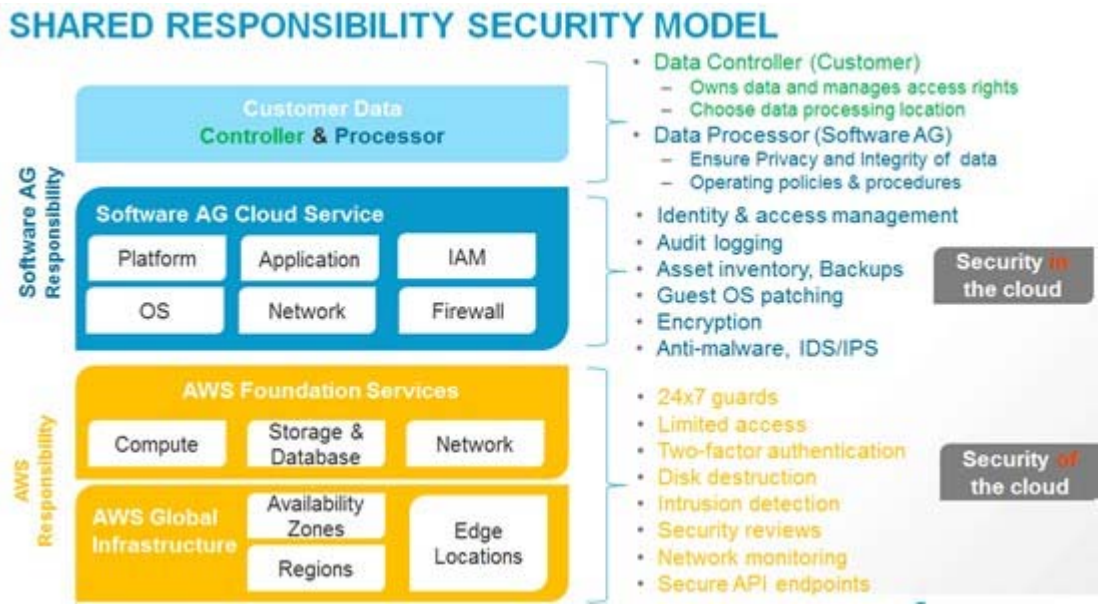
9. Subservice Organization Amazon Web Services (AWS)

AWS Services Description Overview: Software AG 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.

1. AWS provides cloud Infrastructure as a service (IaaS) for Software AG Cloud products including real-time duplication of server infrastructure.
2. AWS provides vulnerability scanning and base hardware patching services as part of their general practices relating to their infrastructure. Any issues noted that could affect any AWS customers, such as Software AG, are reported to them.
3. Physical access to the AWS data centers is strictly controlled and audited according to their ISO 27001 and SOC 2 controls.
4. AWS provides secure data deletion capabilities according to AWS DoD standards. AWS uses the techniques detailed in DoD 5220.22-M "National Industrial Security Program Operating Manual "or NIST 800-88 "Guidelines for Media Sanitization" to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices.

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: Software AG CloudOps 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. The Software AG Cloud Organization complies with 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.

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 located 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-premises 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 Cumulocity IoT Cloud software and for notifications to the Cumulocity IoT CloudOps 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 message 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 Security Hub: AWS Security Hub provides a comprehensive view of high-priority security alerts and security posture across production AWS accounts.

  See https://aws.amazon.com/security-hub/
- 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.

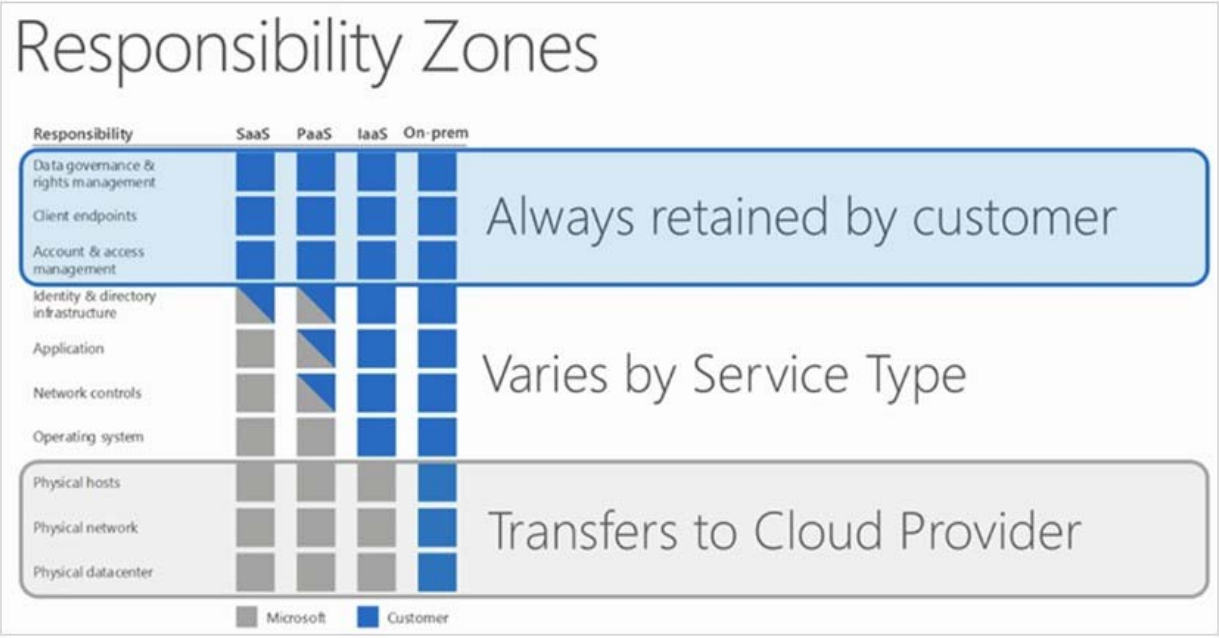
  See https://aws.amazon.com/systems-manager/

10. Subservice Organization Microsoft Azure

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

1. MS Azure provides cloud IaaS for Software AG Cloud products including real-time duplication of server infrastructure.
2. MS Azure provides vulnerability scanning for the underlying Azure-managed infrastructure and cloud network perimeter as well as base hardware patching services as part of their general practices relating to their infrastructure. Any issues noted that could affect any Azure customers, such as Software AG, are reported to them.
3. Physical access to the MS Azure data centers is strictly controlled and audited according to their ISO 27001 and SOC 2 controls.
4. MS Azure provides secure data destruction capabilities when customers delete data or leave Azure. Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.

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), PaaS, and IaaS deployment that Software AG (Customer) is responsible for and Microsoft is responsible for.



Software AG Responsibilities: Software AG CloudOps 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:

Applicable Azure Services

Infrastructure Services

- Azure Virtual Networks: Provide an isolated, private environment in the cloud. Users have control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways.
- Azure Virtual Machines: Virtual servers allow users to deploy, manage, and maintain OS and server software. Instance types provide combinations of CPU/RAM. Users pay for what they use with the flexibility to change sizes. Amazon EC2 provides resizable compute capacity in the cloud.

  See Azure Virtual Machines
- Azure Virtual Machines scale set: Azure virtual machine scale sets let users create and manage a group of identical, load balanced VMs.
- Azure Kubernetes Services: Azure Kubernetes Service (AKS) makes it simple to deploy a managed Kubernetes cluster in Azure. AKS reduces the complexity and operational overhead of managing Kubernetes by offloading much of that responsibility to Azure.
- Azure Container Instances: Azure Container Service allows to quickly deploy a production-ready Kubernetes, DC/OS, or Docker Swarm cluster
- Azure Block Bobs: Object storage service, for use cases including cloud applications, content distribution, backup, archiving, disaster recovery, and big data analytics.
- Azure DNS & Traffic Manager: A service that hosts domain names, plus routes users to Internet applications, connects user requests to datacenters, manages traffic to apps, and improves app availability with automatic failover
- Azure SQL Database, Database for MySQL and Database for PostgreSQL: A globally distributed, multi-model database that natively supports multiple data models: key-value, documents, graphs, and columnar.
- Azure Active Directory Domain Services + Windows Server Active Directory on Azure IaaS: Comprehensive identity and access management cloud solution that provides a robust set of capabilities to manage users and groups. It helps secure access to on-premises and cloud applications, including Microsoft online services like Office 365 and many non-Microsoft SaaS applications.
- Azure Active Directory: Allows users to securely control access to services and resources while offering data security and protection. Create and manage users and groups and use permissions to allow and deny access to resources.
- Azure Storage Service Encryption: Helps organizations protect and safeguard their data and meet their organizational security and compliance commitments.
- Azure Key Vault: Provides security solution and works with other services by providing a way to manage, create, and control encryption keys stored in hardware security modules (HSM).

Security and Monitoring Services

- Azure Advisor: Provides analysis of cloud resource configuration and security so subscribers can ensure they're making use of best practices and optimum configurations.
- Azure Security Center: An automated security assessment service that improves the security and compliance of applications. Automatically assess applications for vulnerabilities or deviations from best practices.

- Azure Defender: A service that provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, the users network, and more.
- Azure Network Security Groups: Used to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.
- Azure Web Application Firewall (WAF): A service that provides real-time protection for web apps.
- Azure Monitor: Provides monitoring for Azure cloud resources.

11. Software AG Cloud platform on Amazon Web Services (AWS)

SAG Cloud Services Specific Description

SAG Cloud is an umbrella product providing a 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. SAG Cloud is not covered by the scope of this report.

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)

SAG Cloud Service Specific Software

- *Linux Operating System:* SAG Cloud server instances are running Linux Operating system and are licensed through AWS on their EC2 service.
- *KeyCloak Database:* KeyCloak database is used for storing subscription details of customers, used for identity and management.
- *Temporal Database:* This database used for storing workflow of the customer environment.
- *Akamai:* Akamai is used for support staff to the bastion hosts for access and troubleshooting operational issues.
- *EKS:* EKS is used for operational and product requirements built in, providing Immutable Infrastructure. EKS uses amazon provided AMIs for Kubernetes cluster.
- *CA3S:* CA3S is used to deploy the infrastructure, consisting of built product AMIs together with supporting infrastructure such as load-balancers and EKS clusters.
- *CAS, Prometheus and Splunk:* CAS, Prometheus and Splunk tools are used for performance, and availability monitoring of customer's Cloud Service components and resources.
- *CLS:* CLS is used for log management and analysis of customer's Cloud infrastructure components and resources.
- *Statuspage:* Statuspage is used for report availability monitoring of customer's Cloud Service components and resources.

  See https://webmethods.statuspage.io/
- *OpsGenie:* OpsGenie to communicate and track alerts about customer's Cloud infrastructure components and resources health.

  See https://softwareag.app.eu.opsgenie.com/

- *Trustside:* Trustside is used for customer communication/notification for report availability monitoring of customer's Cloud Service components and resources.

SAG Cloud Procedures

Customer Onboarding: The following details covers the full SAG Cloud customer onboarding scenario:

- A user goes to softwareag.cloud and signs up for a product
- Fills details in global sign-up page,
  - Block the requests from blocked countries
  - Used domain can't be taken
- On successful validation,
  - Information send to Marketo (Software AG department)
  - Product and IDM are provisioned.
- On successful product provisioning, individual products send e-mail to customer with tenant access details.
- Customer follows the link in e-mail
  - User is redirected to SAG Cloud Login page
  - On successful authentication, user goes back to product.
- User stays back in browser and clicks the Login link of the product
  - User is taken to the signed-up product
- User stays back in browser and clicks the Login link of My cloud
  - User taken to the my cloud page
- User goes to Marketing site and clicks Login
  - User is asked for subdomain and routed to region specific IDM
  - Post login, user is taken to My cloud page
- Tenant Admin logs in (via marketing site and clicks mycloud or mycloud URL) and start user on boarding.
  - User on-boarding triggers an e-mail with change password link which also verifies e-mail.
  - Post password change, user goes to product directly.
- Admin logs in (via marketing site and clicks mycloud or mycloud URL)
  - User administration is shown only to admin
  - Changes the password policy
  - Locks the user account (disable the user in IDM)
  - Admin changes the password and other user details.
  - Can subscribe to a product
    - Only one active trial per product
    - Not more than 3 is allowed
- User logs into My cloud
  - Change password and other user attributes
  - Can see all the subscribed products and can navigate to products
- User is able to switch between marketing content and my cloud content seamlessly
- Marketing site will show mycloud link and user detail at the right post login
- (Optional) In cases of a purchased cloud product (i.e. non-trial), Logistics and RnD update the license limits and expiration date according to the contract.

12. Software AG Cloud platform on Microsoft Azure

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. SAG Cloud is not covered by the scope of this report.

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 SOFTWARE AG Cloud Services Specific Description).

- *KeyCloak Database:* KeyCloak database is used for storing subscription details of customers, used for identity and management.
- *Temporal Database:* This Database used for storing workflow of the customer environment
- *Akamai:* Akamai is used for support staff to the bastion hosts for access and troubleshooting operational issues
- *EKSAKS:* AKS is used for operational and product requirements built in, providing Immutable Infrastructure. AKS uses Azure provided AMIs for Kubernetes cluster. EKS is used for operational and product requirements built in, providing Immutable Infrastructure. EKS uses amazon provided AMIs for Kubernetes cluster.
- *CA3S:* ca3s is used to deploy the infrastructure, consisting of built product AMIs together with supporting infrastructure such as load-balancers and EKS AKS clusters.
- *CAS, Prometheus and Splunk:* CAS, Prometheus and Splunk tools are used for performance, and availability monitoring of customer's Cloud Service components and resources.
- *CLS:* CLS is used for log management and analysis of customer's Cloud infrastructure components and resources.
- *Statuspage*: Statuspage is used for report availability monitoring of customer's Cloud Service components and resources.

  See https://webmethods.statuspage.io/
- *OpsGenie:* OpsGenie to communicate and track alerts about customer's Cloud infrastructure components and resources health.

  See https://softwareag.app.eu.opsgenie.com/
- *Trustside:* Trustside is used for customer communication/notification for report availability monitoring of customer's Cloud Service components and resources.

SAG Cloud Procedures

Customer Onboarding: SAG Cloud customer scenarios in full scope

- A user goes to softwareag.cloud and signs up for a product
- Fills details in global sign-up page
  - Block the requests from blocked countries
  - Used domain can't be taken

- On successful validation,
  - Information send to Marketo (Software AG department)
  - Product and IDM are provisioned.
- On successful product provisioning, individual products send e-mail to customer with tenant access details.
- Customer follows the link in e-mail
  - User is redirected to SAG Cloud Login page
  - On successful authentication, user goes back to product.
- User stays back in browser and clicks the Login link of the product
  - User is taken to the signed-up product
- User stays back in browser and clicks the Login link of My cloud
  - User is taken to the my cloud page
- User goes to Marketing site and clicks Login
  - User is asked for subdomain and routed to region specific IDM
  - Post login, user is taken to My cloud page
- Tenant Admin logs in (via marketing site and clicks mycloud or mycloud URL) and start user on boarding.
  - User on-boarding triggers an e-mail with change password link which also verifies e-mail.
  - Post password change, user goes to product directly.
- Admin logs in (via marketing site and clicks mycloud or mycloud URL)
  - User administration is shown only to admin
  - Changes the password policy
  - Locks the user account (disable the user in IDM)
  - Admin changes the password and other user details.
  - Can subscribe to a product
    - Only one active trial per product
    - Not more than 3 is allowed
- User logs into My cloud
  - Change password and other user attributes
  - Can see all the subscribed products and can navigate to products
- User is able to switch between marketing content and my cloud content seamlessly
- Marketing site will show mycloud link and user detail at the right post login
- (Optional) In cases of a purchased cloud product (i.e. non-trial), Logistics and RnD update the license limits and expiration date according to the contract.

Service Level Reporting

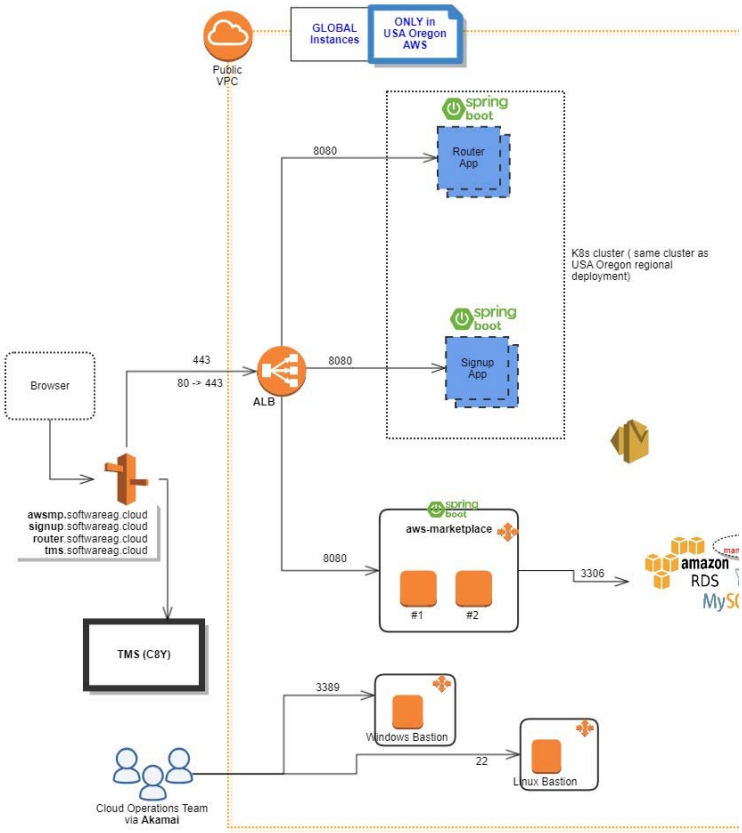
As specified in the cloud contract service attachment, the service availability SLA is 99.5%. The customer can subscribe for notifications on the Software AG Cloud trust site https://trust.softwareag.com/sagcloud/status/.

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.



Service Level Reporting

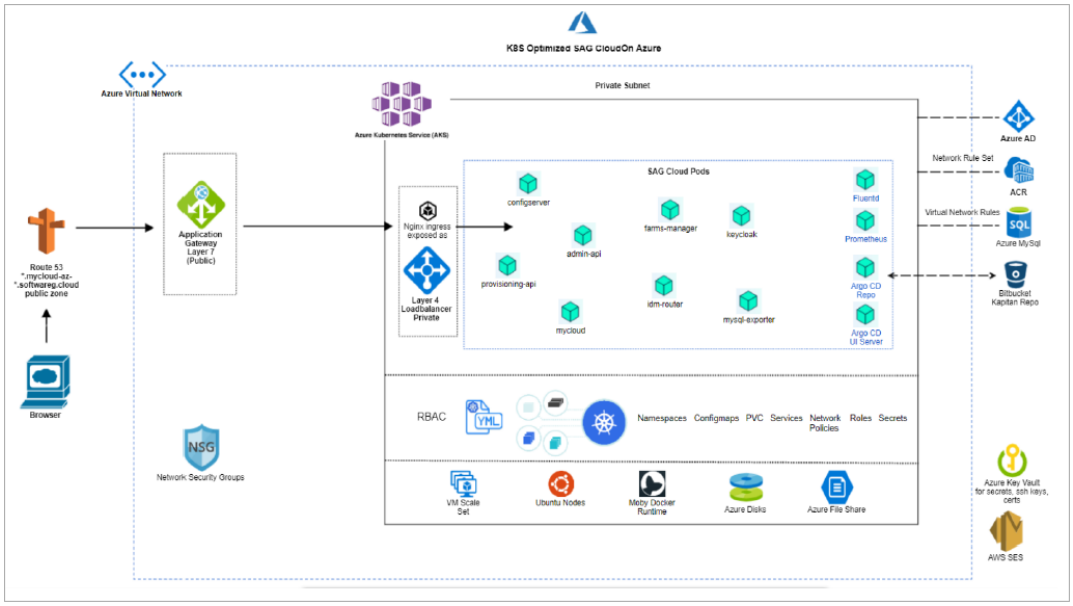
As specified in the cloud contract service attachment service availability is 99.5%. The customer can subscribe for notifications on the Software AG Cloud trust site https://trust.softwareag.com/sagcloud/status/.

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 SOFTWARE AG 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.



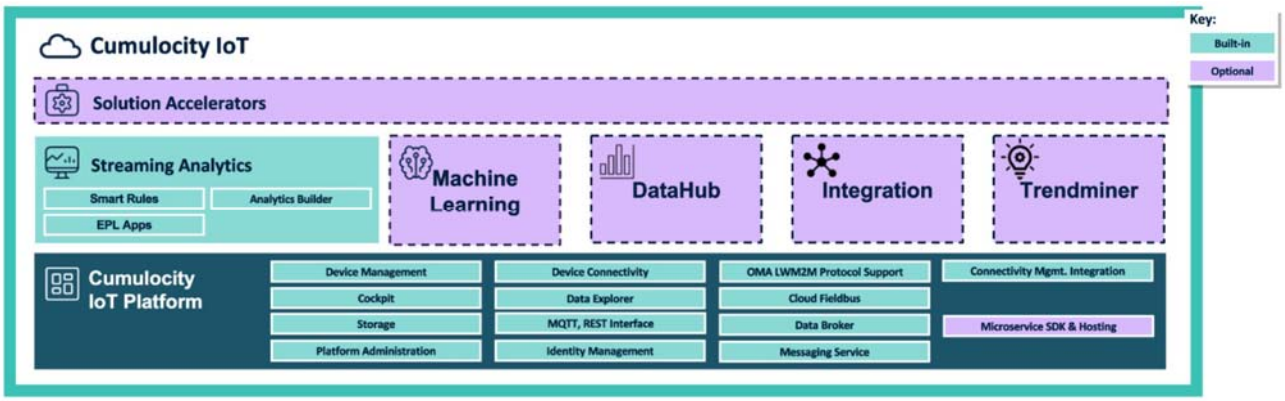
13. Cumulocity IoT Cloud System Services Specific Description

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

Cumulocity IoT is a platform designed for building Internet-of-Things (IoT) / Machine-to-Machine (M2M) solutions. An IoT/ M2M solution enables an end-user to manage and control remote assets that are equipped with sensors (such as GPS devices, electricity meters, and humidity sensors) and actuators (such as switches and valves). The platform has been designed right from the beginning as cloud software. One of the key advantages for end-users is that they do not have to provide, manage, and maintain their own, dedicated computing resources for their IoT/M2M solution. Cloud also means no or significantly lower up-front investments, and very fast deployment. The platform is offered as a fully managed service and is accessible through common Internet browsers on computers, tablets, or smartphones.

Cumulocity IoT Cloud Model

Cumulocity IoT Cloud is offered in two forms. 1. Cumulocity IoT Dedicated Cloud instance setup – Subscription model, 2. Cumulocity IoT Public Cloud - SaaS model



Cumulocity IoT Base Platform Features

Administration Application

- Enables account administrators to manage their users, roles, tenants, applications, business rules, and lets them configure a number of settings for their account.
- Features include:
  - Home Screen to view statistics
  - View audit logs
  - Manage users and their roles
  - Manage Applications
  - Manage Tenants (also for subtenants)
  - Set up Two-factor authentication
  - Standard 3 availability zone setup
  - Real-time event processing for your Business Rules
  - Manage your Data Retention
  - Manage the Data Broker

Cockpit Application

- Includes options to manage and monitor IoT assets and business data.
- Features include:
  - Data explorer: Interactively explore, compare and visualize IoT data
  - Dashboards: Create your own pages by freely selecting and arranging widgets. Select from various widgets including maps, tables, graphs, charts, controls, and more
  - Business Rule Package (Smart Rules): Easily create business rules to perform actions on incoming data in real-time. Use predefined business rules for geofencing, thresholds or alarm escalation and notifications (SMS/Email)
  - Reporting: Create reports based on dashboards layout and send distribute them by Email
  - Asset Management: Organize your connected assets in hierarchies
  - Alarm Management: Monitor problems of your asset using severities and workflows
  - Get on introduction and overview using the Welcome Dashboard and Home Dashboard, respectively.
  - Organize thousands of devices using groups

Device Management Application

- Provides functionalities for managing and monitoring devices and enables you to control and troubleshoot devices remotely.
- Features include:
  - Device Management
    - Device Lifecycle
    - Device Twin
    - Device Inventory & Runtime Statistics
    - Device Identity Management
    - Credentials per individual device
    - Provisioning for small & large deployment
    - Auto-registration
    - Asset management (network, location, etc.)
    - Gateway hierarchy and command routing

  - Connection Management
    - Connection availability monitoring
    - Connect metrics (RSSI, Signal Strength)
  - Firmware & software management
    - Fault & alarm management
    - Configuration management
    - Remote command execution
    - Bulk operations with scheduling
    - Troubleshooting: Remote shell, logs, etc.
    - Real-time alarms with integrated workflow
  - Device application It offers the following functionality:
    - Basic mode with minimal data entry requirements
    - Expert mode to specify asset location, reference configuration, and more
    - Detailed status visualization to identify connection problems
    - Scan identity directly from the device using a barcode scanner
    - Support of Cumulocity multitenant device bootstrap

Cumulocity IoT DataHub Application

- Cumulocity IoT DataHub gives you open access to historical IoT data for analytics. DataHub extracts data on a scheduled, incremental basis from the Cumulocity IoT platform and optimizes and stores it for analytical queries in a data lake.
- The main features are:
  - It allows the use of scalable and inexpensive storage by providing an easy-to-use data pipeline that extracts data from the Operational Store of Cumulocity IoT, transforms the data into a relational format, and stores it in a data lake of customers choice for both long term archival and efficient analytical querying.
  - It offers an SQL-based Query Interface for querying the data lake and enables the connection of arbitrary applications that support ODBC, JDBC, or REST protocols.
- The important components are
  - Cumulocity IoT DataHub Web Application: The DataHub Web Application is the graphical user interface that allows the user to set up and configure DataHub and its offloading pipelines.
  - Cumulocity IoT DataHub Microservice: The DataHub microservice is responsible for scheduling the extraction from data into the data lake and handles the requests by the DataHub webApp.
  - Cumulocity IoT DataHub Engine (Dremio): Scalable SQL engine which is both used for extracting data from the platform into data lakes and for efficient analytic querying.
  - Databases: Both the DataHub Microservice and the DataHub Engine require a database for persisting their metadata.
  - Data Lake: Storage container for offloaded data either on the basis of ADLS Gen2/Azure
  - Storage (Azure), S3 (Amazon), NAS, or HDFS
- More details at https://cumulocity.com/guides/datahub/datahub-overview

Streaming Analytics Application

- Cumulocity IoT Streaming Analytics provides real-time analytics, management, and monitoring of live streaming data within the Cumulocity IoT platform.

- Cumulocity IoT uses the Apama streaming analytics engine for the design, development, and deployment of sophisticated Complex Event Processing (CEP) applications that can monitor event streams, detect and analyze event patterns, and take actions immediately.
- Cumulocity IoT Streaming Analytics delivers:
  - Smart Rules - a wizard-driven approach for creating simple rules that monitor devices and raise alarms
  - Analytics Builder - a drag and drop environment for building advanced models that analyze multiple measurements using a library of analytics
  - EPL Apps - a coding environment for developing complex and sophisticated applications
  - using a powerful event-based language
- Streaming analytics is executed in an "Apama-ctrl" microservice which has a per-tenant isolation scope. This means that each subscribed tenant has its own instance of the microservice container with dedicated resources (memory and CPU usage). The container is isolated from other tenants, and therefore high CPU load or memory issues for one tenant are tracked and resourced independent of other tenants.
- More details at https://cumulocity.com/guides/apama/overview-analytics/

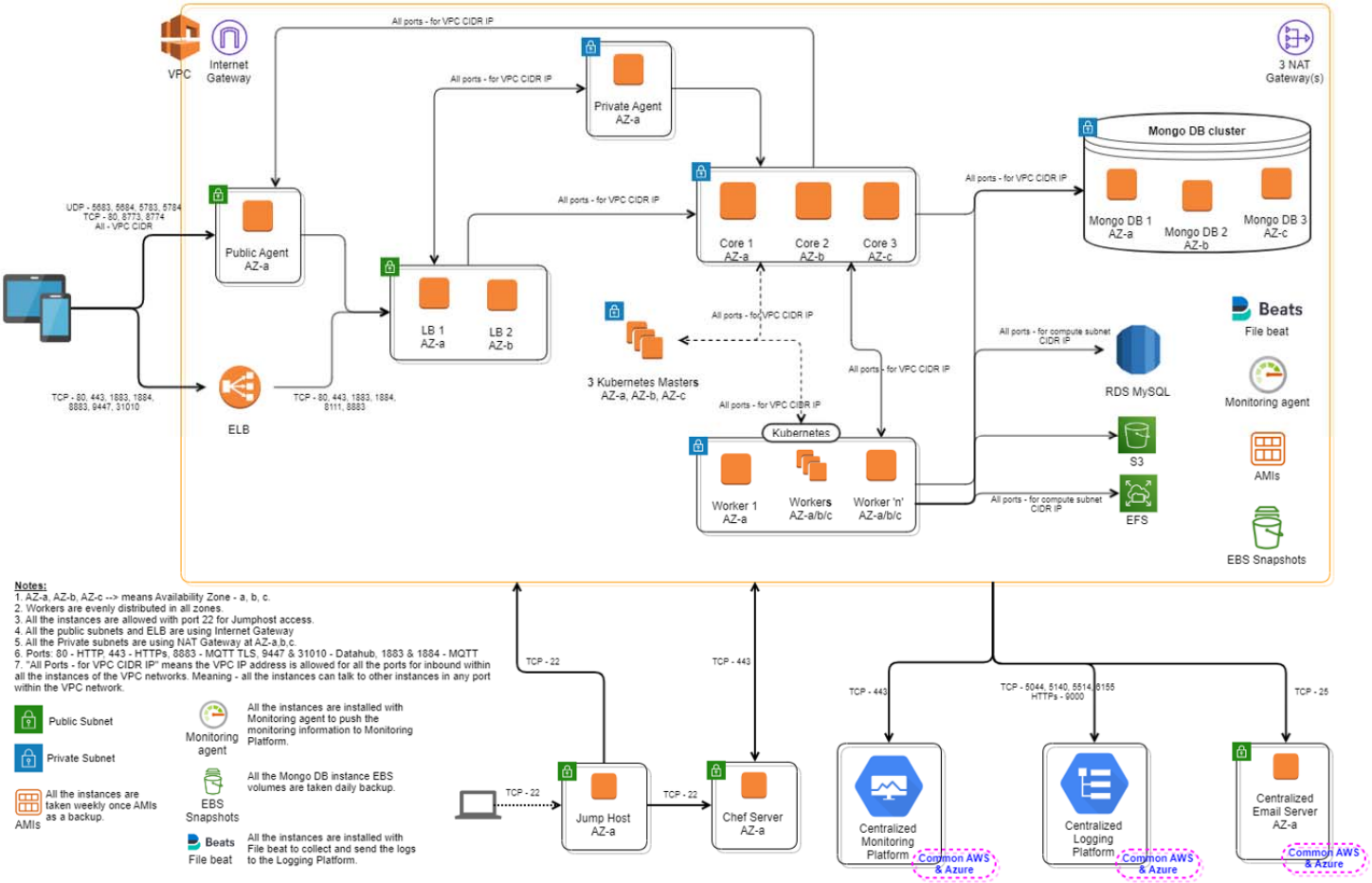
Machine Learning Workbench Application

- Machine Learning Workbench (MLW) enables data scientists and machine learning engineers to build, train, and evaluate high-quality machine learning models using an intuitive, easy-to-use, no code Graphical User Interface and a programmer friendly Jupyter Notebook based environment.
- MLW provides seamless access to data residing in Cumulocity IoT operational store or any cloud data lakes with visual tools to ingest and transform the data.
- MLW is aimed at data scientists and machine learning practitioners to help them solve business problems faster by streamlining the machine learning lifecycle including data capture and analysis, model training and evaluation, and model deployment.
- More details are available in the Cumulocity IoT Machine Learning Guide: https://cumulocity.com/guides/machinelearning/introduction/

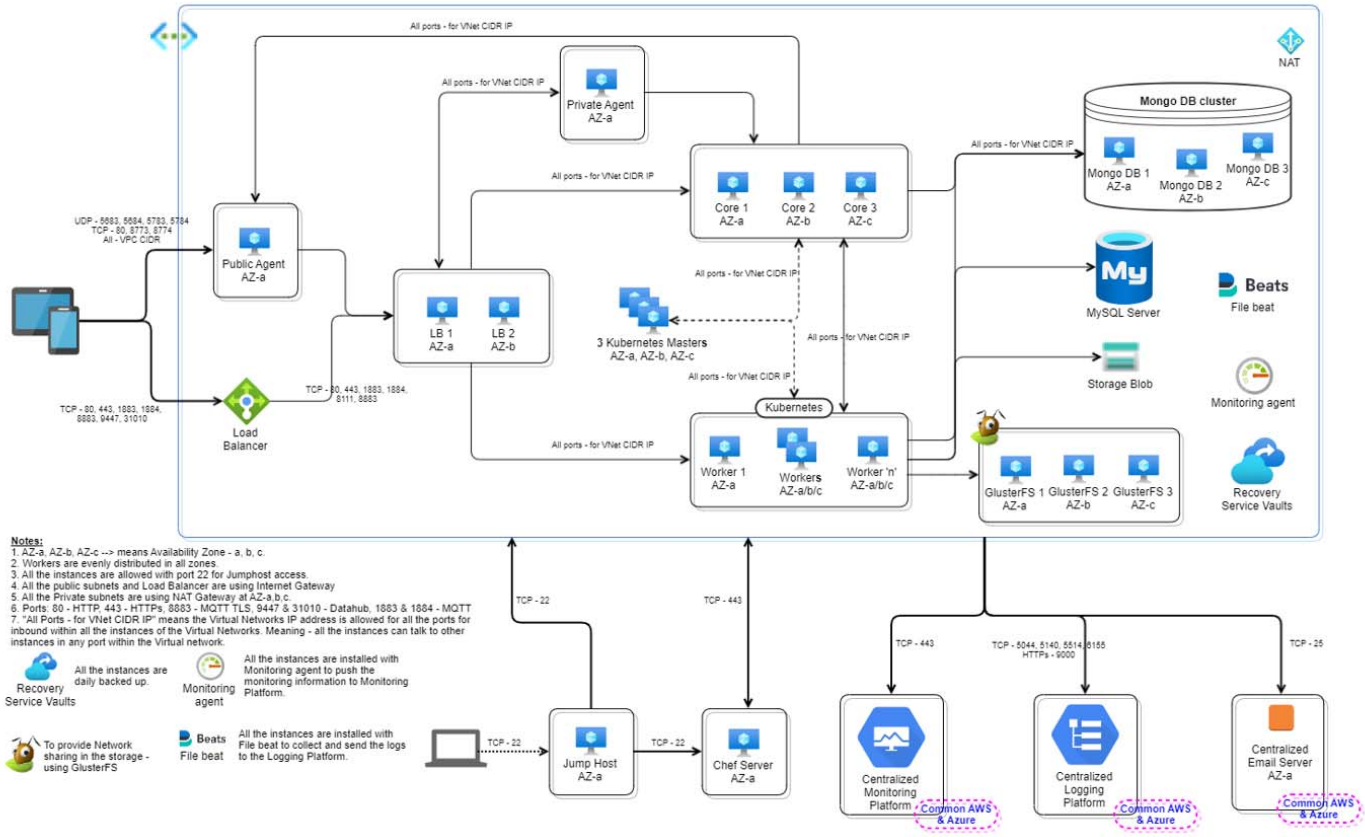
Machine Learning Engine Application

- Machine Learning Engine (MLE) enables machine learning/IT operators to manage and operationalize production-ready models for generating predictions on data gathered from connected devices. These capabilities can be leveraged either from a web browser via an easy-to-use graphical user interface or programmatically via REST API.
- MLE provides a high-performance inference platform with deployed models exposed as endpoints that can be leveraged from Streaming Analytics and other applications for real-time inference.
- MLE supports models represented in PMML and ONNX formats. It also provides you insights into your models by capturing runtime performance and showcasing it via meaningful KPIs.
- MLE allows you to create model groups, manage custom resources which your models might need, create inference pipelines by combining custom pre-processing and post-processing code with relevant models, and schedule batch jobs for processing measurements from devices or device groups against an available model or model group.
- More details at Cumulocity IoT Machine Learning Guide: https://cumulocity.com/guides/machinelearning/introduction/

Cumulocity IoT Cloud Platform Architecture



Microsoft Azure Cloud Architecture of Cumulocity IoT Platform



Cumulocity IoT Specific Software

- **Linux Operating Systems:** Cumulocity Cloud server instances are running Linux Operating Systems and are licensed through AWS on their EC2 service.
- **MongoDB:** MongoDB is used as the Database Management System for the Cumulocity IoT Platform.
- **Kubernetes:** Kubernetes is used in the underlying infrastructure to host functional extensions to the platform in the form of microservices. It orchestrates the microservice lifecycle of the containers that host the microservices. Please see https://kubernetes.io/ for details.
- **Graylog:** Graylog is used for log management and analysis of customer's Cloud infrastructure components and resources. More details at https://www.graylog.org/

Product Enhancements

- Customers may submit suggestions or product enhancements via Cumulocity IoT Ideas.

Cumulocity Cloud Data

- As specified in the cloud contract service attachment the system provides a Recovery Point Objective of 24 hours and a Recovery Time Objective of 12 hours.
- Further details are provided in the internal Results of Cumulocity Disaster Recovery cloud operations documentation.

Cumulocity IoT Selling Packages

- Cumulocity IoT Platform is being sold in multiple packages. Below is a high-level overview of them.

Name of application	Public Cloud - Partners	Public Cloud - Trial	Public Cloud - Basic - IOTPB	Public Cloud - Advanced - IOTPA	Dedicated Cloud - IOTPD
Administration	Yes	Yes	Yes	Yes	Yes
Cockpit	Yes	Yes	Yes	Yes	Yes
Device Management	Yes	Yes	Yes	Yes	Yes
Device-simulator	Yes	Yes	Yes	Yes	Yes
Apama-ctrl-starter	-	-	-	-	-
Smartrule	Yes	Yes	Yes	Yes	Yes
Apama Analytics Builder	Yes	Yes	Yes	Yes	Yes
Feature-fieldbus4	Yes	Yes	Yes	Yes	Yes
Connectivity-agent-server	Yes	Yes	Yes	Yes	Yes
Cloud-remote-access	Yes - on demand	-	Yes - on demand	Yes - on demand	Yes - on demand
Lwm2m-agent	Yes - on demand	-	Yes - on demand	Yes - on demand	Yes - on demand
Opcua-mgmt-service	Yes - on demand	-	Yes - on demand	Yes - on demand	Yes - on demand
Sigfox-agent	Yes - on demand	-	Yes - on demand	Yes - on demand	Yes - on demand
Actility	Yes - on demand	-	Yes - on demand	Yes - on demand	Yes - on demand
DataHub	Yes - Upon approval	-	-	Not available	Yes - but pay for it.
Feature-microservice-hosting	-	-	Paid	Paid	Paid
Zementis-* (and) Predictive Analytics (machine-learning) (and) Nyoka (and) Onnx	-	-	-	Paid	Paid
Apama-ctrl-* (and Apama EPL apps together)	-	-	-	Yes - 1c-4g	Yes - 1c-4g
Feature-branding	-	-	-	Yes	Yes
Feature-broker (data broker)	-	-	-	Yes	Yes
Feature-user-hierarchy	-	-	-	Yes	Yes
Sslmanagement	-	-	-	Yes	Yes
Allow sub tenant creation (check box)	-	-	-	Paid	Paid
Report-agent	Yes	Yes	Yes	Yes	Yes
Machine Learning Workbench with	-	-	-	paid	paid

Name of application	Public Cloud - Partners	Public Cloud - Trial	Public Cloud - Basic - IOTPB	Public Cloud - Advanced - IOTPA	Dedicated Cloud - IOTPD
MLW (or) MLW-CDH					

Cumulocity IoT Dedicated Cloud Instance

Cumulocity IoT Cloud Platform Architecture

- Cumulocity IoT Dedicated Cloud instance setup is offered in AWS and Azure Cloud providers. The setup is by default distributed across three availability zones of a given cloud provider region.
- By default, the architecture allows operational continuity of the platform for the failure of one availability zone due to highly available architecture and design.
  - Monitoring informs the CSO team in case of any failures.
  - The agent node is a single virtual machine setup due to its functional nature. However, this can be redeployed in another available zone quickly upon failure notification alarm.
- For dedicated instances of Cumulocity IoT, any AWS or Azure region can be chosen by the customer according to their business need and locality.

Cumulocity IoT Cloud Procedures

Onboarding Customers

- Tenant creation in Cumulocity IoT Dedicated Cloud Instance is managed by the customer who is the tenant owner as the whole Cumulocity IoT Platform belongs to the customer. The underlying infrastructure and the components are being set up, monitored, and maintained by CSO.
- A detailed email is sent by the Logistics team with the SAP signed Contract, materials to be provisioned, license key, and the Questionnaire Template (Questionnaire Dedicated Cloud instance setup) to be completed by Sales or the Customer, is sent to cc-operations@softwareag.com email address.
  - Then setup is executed by CSO as per the above architecture specifications.
  - Only the initial users for the customers in the management tenant are created and then delivery is complete.
- Delivery quality is executed by verifying against the checklist (Template - Cloud Ops Engineer Checklist) for Dedicated Cloud instance setup.

Service Level Reporting

- As specified in the cloud contract service attachment service availability is 99.9%.
- Customers will be provided service reports on request.
- Some customers setup an SLA portfolio on an on-demand basis which is similar to: http://status.cumulocity.com/

Change Management

- All changes (e.g., upgrades) will be mutually agreed upon between the platform owner (customer) and Cumulocity IoT cloud operations by following the release processes and guidelines.

Cumulocity IoT Public Cloud SaaS

Cumulocity IoT Cloud Platform Architecture

- Cumulocity IoT Public Cloud SaaS setup is offered in AWS and Azure Cloud providers. The setup is by default distributed across three availability zones of a given cloud provider region.
- By default, the architecture allows operational continuity of the platform for the failure of one availability zone due to highly available architecture and design.
  - Monitoring informs the CSO team in case of any failures.
  - The agent node is a single virtual machine setup due to its functional nature. However, this can be redeployed in another available zone quickly upon failure notification alarm.
- At AWS cloud provider, Cumulocity IoT Platform is offered in the following regions:
  - US West (Oregon) Region
  - Europe (Frankfurt) Region
  - Asia Pacific (Sydney) Region
- At Azure cloud provider, Cumulocity IoT Platform is offered in the following region:
  - West Europe (Netherlands) Region

Cumulocity Cloud Procedures

Onboarding Customers

Internal Tenants

- Internal tenants are used by SAG personnel for technical purposes like monitoring, development, demonstration, POC purposes, etc. They do not contain customer specific data.
- Responsible for the creation of such tenants is Cloud Service Operations
- Tenants are created after an email received at cc-operations@softwareag.com or an iTrac work item has been created defining the following items:
  - URL, Desired tenant ID, Contact name, Contact email, Required applications to subscribe, Cost center (unless the tenant is internal to CSO)
- They are documented via the Additional Features - Cumulocity IoT Public Cloud Customers posted on the Software AG iWiki website.
- The tenant is created in the management tenant of the request Cumulocity IoT Platform. Credentials are automatically sent to the tenant admin contact given in the request.

Trial Tenants

- Trial tenants are tenants for customers to evaluate the functionality of Cumulocity IoT SaaS features.
- The provisioning of the tenants is possible by anyone in the world at Software AG Cloud www.softwareag.cloud platform by choosing Cumulocity IoT Cloud product.
- The life cycle of the tenant is being controlled by the Software AG Cloud www.softwareag.cloud platform for the Cumulocity IoT product. Like creation, suspension, extension, and deletion.

Commercial Tenants

- Commercial tenants are customer tenants which are created in the Public Cloud Offering of Cumulocity IoT SaaS Platform.
- A detailed email with the following information is sent to cc-operations@softwareag.com email address - the CSO team by the Software AG Logistics team.
  - SAP signed Contract,
  - Product Materials to be provisioned,
  - License key, and

  - The latest Questionnaire form from the Template (Questionnaire Public Cloud setup) to be completed by Sales or the Customer
- The tenant is created in the management tenant by the CSO team then.
- Credentials are automatically sent to the tenant admin contact given in the request while creating the tenant.
- The tenant life cycle is based on the SAP signed contract. Like creation, suspension, extension, and deletion.

Public Cloud SaaS Offering

The following are public cloud Cumulocity IoT cloud offerings:

	Cumulocity IoT Platform	Cloud Provider and Region	Commercial	Trial	www.softwareag.cloud
1	https://management.cumulocity.com/	AWS Europe (Frankfurt) Region	Yes	-	-
2	https://management.apj.cumulocity.com/	AWS Asia Pacific (Sydney) Region	Yes	-	-
3	https://management.us.cumulocity.com/	AWS US West (Oregon) Region	Yes	Yes	Yes
4	https://management.emea.cumulocity.com/	Azure West Europe (Netherlands) Region	Yes	-	Yes
5	https://management.eu-latest.cumulocity.com/	AWS Europe (Frankfurt) Region	-	Yes	Yes

D. Principal Service Commitments and System Requirements

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

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

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

E. Non-Applicable Trust Services Criteria

Common Criteria (CC)		
Non-Applicable Trust Services Criteria		**Software AG Cloud's Rationale**
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	N/A – The Company's IaaS provider is responsible for physical and environmental security controls.

F. Subservice Organizations

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

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

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Amazon Web Services (AWS)	The Company uses Amazon AWS Elastic Compute Cloud (Amazon EC2) for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses the Amazon Relational Database Service (Amazon RDS) and AWS Simple Storage Service (S3). Amazon RDS is a Platform-as-a-Service or more specifically a Database-as-a-Service. AWS S3 provides object storage through a web service interface. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls around the underlying infrastructure and Data Centers supporting the In-Scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure such as physical servers and physical access to backups and facilities; • Controls around the S3 databases, including controls around physical access to the backup servers and facilities, high availability replication, physical access to storage systems, operating system installation and patches, database software installation and patches, and system configuration;	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.8* CC 7.5* CC 8.1* CC 9.1* A1.1* A1.2* A1.3*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over the Amazon RDS including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; • Controls over managing AWS Platform-as-a-Service components such as physical servers and operating systems including applying critical patching for this infrastructure; • Controls around the change management processes for the AWS Infrastructure-as-a-Service Platform and Azure Platform-as-a-Service Platform components as applicable. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On a quarterly basis, CloudOps selects a customer's full backup for each product to verify the integrity of the backup data. • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the In-Scope production environment and reviews the third parties' System and Organization Control reports such as SOC 2 reports or other related security evaluations. Corrective actions are taken, if necessary.	
Microsoft Azure	The Company uses Microsoft Azure for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses the Azure SQL Database and/or SQL Managed Instance service, which is a Platform-as-a-Service or more specifically a Database-as-a-Service. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls around the underlying infrastructure and Data Centers supporting the In-Scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure such as physical servers and physical access to backups and facilities; • Controls around Azure Storage redundancy, including controls over data replication, physical access to storage systems, system installation and patching, and system configuration; • Controls over the monitoring of the Office 365 / OneDrive Software-as-a-Service components including backups, anti-virus, and incidents related to security and availability including responding to items identified; • Controls over the SQL Database and SQL Managed Instance including database backups, operating system installation and patches, encryption, database software installation and patches, and routers/firewalls monitoring and maintenances; • Controls over managing Azure Platform-as-a-Service components such as physical servers and operating systems including applying critical patching for this infrastructure; • Controls around encryption related to Azure; and	CC5.2* CC6.1* CC6.2* CC6.3* CC6.4 CC6.8* CC7.5* CC8.1* CC9.1* A1.1* A1.2* A1.3*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls around the change management processes for the Azure Infrastructure-as-a-Service Platform and Azure Platform-as-a-Service Platform components as applicable. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On a quarterly basis, CloudOps selects a customer's full backup for each product to verify the integrity of the backup data. • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the system and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.	

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

G. User Entity Controls

Software AG's controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary user entity controls identified within the table below, where applicable. As applicable, suggested control considerations and/or complementary user entity controls and their associated criteria have been included within the table below.

Management has highlighted criterion in which complementary user entity controls were assumed in the design of the Company's system with an asterisk. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes each user organization should consider in developing their internal controls or planning their audits that are relevant to the Company's controls detailed in this report, however, such control considerations are not required to achieve design or operating effectiveness for the Company's service commitments and system requirements based on the applicable trust services criteria. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user entity. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities which provide a basis for the assertions underlying the control environments for the Company's user entities.

User Entity Control	Associated Criteria
User entities are responsible for 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.	CC 1.3 CC 6.5
User entities are responsible for immediately notifying Software AG of any actual or suspected information security breaches, including compromised user accounts.	CC 2.3
User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with the cloud systems.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.7
User entities are responsible for access control to the tenant application and may grant CloudOps personnel access providing user credentials, function privileges, and client license to access the data.	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.7*
User entities are responsible for establishing logical security controls to restrict and monitor access to cloud systems.	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.7*
User entities are responsible for end-user administrative privileges within their cloud tenant and have control over who is authorized to access their environment, including adding, changing, and removing user access.	CC 5.2* CC 6.1* CC 6.6* CC 6.7* CC 6.8*

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


Aprio